HUMAN SCIENCES AND CULTURES.

SOCIETY, EDUCATION, POLITICS, AND COMMUNICATION (XXXVII CYCLE 37) -

POLITICS, LAW, MARKET CURRICULUM - AT THE UNIVERSITY OF SALERNO

Department of Political Sciences and Communication/DISPC

Ph.D. Thesis by Mohammad ZAREE

Title: Blockchain for Anti-Corruption: A Comparative Study of Legal, Regulatory, and Technological Approaches in Public Procurement in Italy, Canada, and the United States.

Supervisor: Associate Professor Roberta Troisi

Submitted: September 2025

Abstract

This dissertation investigates the potential of blockchain technology as an architecture for reducing corruption in public procurement in a comparative context in three jurisdictions—Italy, Canada, and the United States. Corruption can happen anywhere in public procurement, especially where there are systems in place that break down hierarchically or where legal ambiguity reduces deterrence. There has been much exploration of blockchain as a paradigm shift for promoting transparency, traceability, and greater levels of automation throughout the procurement procedure. However, literature on blockchain technology for public procurement is mainly techno-focused, with scant attention paid to the myriads of legal-regulatory constraints that will shape implementation outcomes, especially within a normative framework like public procurement, in disparate governance systems.

To address this gap, this study develops a three-dimensional analytical lens—governance transformation, legal-regulatory adaptation, and institutional readiness—to examine the feasibility of deploying blockchain technology in public procurement systems. This study follows a doctrinal legal approach and uses a qualitative comparative analysis lens to examine legislative frameworks, procurement systems, and blockchain initiatives at the jurisdictional level, using statutory texts, regulatory agency documents, procurement transparency indexes, and implementation case studies as data sources.

The study's findings show that while blockchain technology has the potential to mitigate corruption in the public procurement context, it is not universal or automatic, and would be shaped by jurisdiction-specific conditions. While Italy has centralized procurement oversight, it conforms to mandated compliance processes through a plethora of legal-based instruments; descriptions of blockchain provide opportunities for efficiency and complexity, Canada’s moderate institutional readiness limits its potential, because of the provincial-federal asymmetries. The United States has immense technological prowess but is limited in terms of regulatory pluralism and lack of interoperability.

This dissertation supports a view that sustainability of blockchain technology for public procurement, depends on flexible legal frameworks; institutional and regulatory coordination, and digital identity and contract standards.

This study builds an interdisciplinary conversation bridging law and technology, furthering the study of digital governance and providing a policy useful framework to assess and support systemic anti-corruption through blockchain in complex public procurement contexts.

Table of contents

Table of Figures

List of Abbreviations

AAL / IAL / FAL	Authenticator / Identity / Federation Assurance Levels
ANAC	Autorità Nazionale Anticorruzione (Italy's National Anti-Corruption Authority)
ATIA	Access to Information Act (Canada)
BDNCP	Banca Dati Nazionale dei Contratti Pubblici (Italy)
CAD	Codice dell'Amministrazione Digitale (Italy's Digital Administration Code)
CANADA Buys	Federal e-tendering portal (SAP Ariba)
DLT	Distributed Ledger Technology
DFARS	Defense Federal Acquisition Regulation Supplement (U.S.)
DIACC	Digital ID & Authentication Council of Canada
eForms-IT	Italian localization of EU e-procurement data forms
eIDAS	Electronic Identification, Authentication and trust Services (EU)
ESIGN	Electronic Signatures in Global and National Commerce Act (U.S.)
EUDI Wallet	European Digital Identity Wallet
FAR	Federal Acquisition Regulation (U.S.)
FOIA	Freedom of Information Act (U.S.)
FRE	U.S. Federal Rules of Evidence
FVOE	Fascicolo Virtuale dell'Operatore Economico (Italy)
GCKey	Government of Canada credential
GDPR	General Data Protection Regulation (EU)
MFA	Multi-Factor Authentication
NIST SP 800-63-3	Digital Identity Guidelines (U.S.)
OJ	Official Journal of the European Union
PAD	Piattaforme di Approvvigionamento Digitale (certified digital procurement platforms, Italy)
PCP	Piattaforma dei Contratti Pubblici (Italy)
PCTF	Pan-Canadian Trust Framework
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PNR	Piano Nazionale di Ripresa e Resilienza (Italy's Recovery Plan)
PSPC	Public Services and Procurement Canada
ReGiS	Italy's PNRR monitoring/registry platform
RPCT	Responsabile della prevenzione della corruzione e della trasparenza (Italy)
RRF	Recovery and Resilience Facility (EU)
RTD	Rappresentante per la Transizione al Digitale (Italy)
RUP	ResponsabileUnico del Progetto (Italy)
SAM.gov	System for Award Management (U.S.)
TBS	Treasury Board of Canada Secretariat
UETA	Uniform Electronic Transactions Act (U.S. states)

Table of Statutes

European Union

Directive 2014/24/EU on public procurement.

Regulation (EU) 2016/679 (GDPR).

Regulation (EU) 2021/241 establishing the Recovery and Resilience Facility (RRF).

Regulation (EU) 2023/2854 (Data Act), Art. 36 (smart-contract safeguards).

Regulation (EU) 2024/1183 (European Digital Identity).

Regulation (EU) No 910/2014 (eIDAS).

Regulation (EU, Euratom) No 883/2013 (OLAF investigations).

Markets in Crypto-Assets (MiCA) Regulation (referenced generally).

Italy

Decreto legislativo 31 marzo 2023, n. 36 (Codice dei contratti pubblici).

Decreto legislativo 10 marzo 2023, n. 24 (whistleblowing—Directive 2019/1937).

Decreto-legge 30 aprile 2022, n. 36 (converted by Law 79/2022) — PNRR acceleration & compliance.

Decreto-legge 14 giugno 2021, n. 82 — establishes the National Cybersecurity Agency.

Legge 11 febbraio 2019, n. 12 (art. 8-ter) — recognition of DLT/smart contracts.

Decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale), art. 17.

ANAC Delibera n. 263/2023 — publication/transparency obligations under the new Code.

Canada

Access to Information Act, R.S.C., 1985, c. A-1.

Canada Evidence Act, R.S.C., 1985, c. C-5 (ss. 31.1–31.8).

Financial Administration Act, R.S.C., 1985, c. F-11.

Government Contracts Regulations, SOR/87-401.

Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.

Secure Electronic Signature Regulations, SOR/2005-30.

Québec: Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR c A-2.1.

Québec: Act Respecting Contracting by Public Bodies, CQLR c C-65.1.

United States

Freedom of Information Act (FOIA), 5 U.S.C. § 552.

Privacy Act of 1974, 5 U.S.C. § 552a.

Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. ch. 96.

Federal Acquisition Regulation (FAR) — electronic commerce, 48 C.F.R. Subpart 4.5.

Procurement Integrity Act, 41 U.S.C. §§ 2101–2107.post-employment restrictions, 18 U.S.C. § 207.

GAO Bid Protest Regulations, 4 C.F.R. pt. 21.

1. Introduction

1.1 Background to the Research Problem

1.1.1. The Global Epidemic of Corruption

Corruption continues to be a significant global challenge that has substantial implications for governance and democracy, economic development and growth, and public trust. Estimates of the economic impacts of corruption have ranged from hundreds of billions of dollars to trillions of dollars each year that deprives society of good quality and fair access to health, education, public infrastructure, and integrity in public institutions (Tanzi, 1998; Dimant & Tosato, 2018). These effects are not only financial. Corruption fundamentally lowers the legitimacy of governments and undermines governments' responsibilities to govern. In its purest form, corruption impacts the reported significantly far beyond abstract policies and programs; it affects the people who suffer a loss of material advantage for society; it reduces the capability of societies to innovate; and it reduces capacity of average citizens to trust in their own laws and the rule of law process.

Corruption has been a defining challenge of the twenty-first century, continually spilling across national borders and beyond formal or informal institutions. Adesola et al. (2024) refer to it as a structural epidemic that very nearly infuses all forms of society, and is resilient to cultural, legal, religious, or occupational cleavages and categorizations. The idea that corruption is specifically an issue of low-income or fragile states is ahistorical. Cross-national studies have demonstrated systemic vulnerabilities across national corruption even within high-income democracies, particularly in public procurement where discretionary budgets are large, legislation is complex, procurement networks are opaque, and formidable (sometimes legal) entry barriers exist for suppliers (Garcia, 2019; Liu & Mikesell, 2014; Ahmadjonov, 2025). In public procurement, corruption directly undermines the principle of equal access to public contracts and erodes public confidence in the fairness of institutions.

While measuring corruption is in principle challenging, Franzoni (2025) indicates present-day global indices do not begin to adequately measure the most hidden aspects of corruption especially in procurement networks where illicitly manipulated contracts and awards are never reported or tagging along with organizations where audit and/or evaluation procedure are truncated. This deficit in measurement, as indicated by Heywood and Rose (2014), makes comparative research and policy design more difficult and underestimating the problem in systemic scope inevitable. However, we have data that indicates institutional degeneration is widespread: Judge, McNatt and Xu (2011) did a meta-analysis of the literature in studying corruption and reported that national corruption levels are strongly correlated to weak rule of law, developing civil service conditions and fragmentation in oversight institutions—all of which exacerbated procurement risk. Corruption is a sort of hidden tax that works macroeconomically to distort resource allocation, reduce productivity, and undermine national competitiveness (Mo, 2001; Enste & Heldman, 2018). In low- and middle-income countries that have less room in public budgets, the economic damage

is compounded, and the impact of irregularities in procurement, such as shoddy infrastructure or inflated contract prices, can directly affect service delivery or development results (Akçay, 2006; Annisa & Lavides, 2025). The combination results in both a crisis of underdevelopment and of public cynicism, where institutions that are supposed to serve the public trust are perceived as only facilitating illicit enrichment and elite favoritism (Ahmadjonov, 2025; Muhammad et al., 2023).

The variety and adaptability of corruption forms within procurement systems are difficult to identify. Corruption in procurement can take many forms; bribery, kickback schemes, bid rigging, favoritism, collusive tendering, outright theft, as well and different obstructions to bidding. In his study, Graycar (2015) emphasizes the need to regard aspects of corruption as more than acts of criminal behavior, but instead as habits of blighted institutions, often made legitimated through informal practices and weak systems of accountability, both within procurement chains. For example, Liu and Mikesell (2014) have demonstrated how corrupt behavior from public officials' incentives manipulation can affect the procurement spending not only by amount spent, but also who receives which contract and what sort (for example, directed public interest projects vs. politically favorable or private interest projects).

Corruption in procurement processes simultaneously reflects more systemic patterns of institutional and political economy. As we discussed in the first chapter, Rose-Ackerman (1996) clarified that public officials are handed wide discretion to manage large contracts of public money, with little oversight through the state. Unchecked public officials have the kind of environment in which to maximalize rents. In another article (2005), she explored when the administrative control systems were fragmented or weak, it still failed to sufficiently discourage engagement in such behaviors. This was often even more so in complex organizational models like infrastructure procurement or public-private partnerships. These risks are not theoretical. Garcia (2019) provided evidence on how procurement for the health sector as drug supply chain management and the purchase of hospital equipment, repeatedly experiences inflated pricing or kickbacks that compromise the fiscal efficiency of health services and public welfare.

More recent work, focusing exclusively on procurement in global food systems, reinforce these findings. Demeshko et al. (2024) argue that procurement decisions have been influenced by collusion and disordered accountabilities by elites. The outcomes are unfulfilled procurement commitments, price overruns, and delivery delays. To simply call these economic inefficiencies ignores the structural undermining of public trust. Several authors emphasize that procurement is arguably the most recognized area for potential corruption in the public sector around the globe, meaning regardless of country income level or agency governance, procurement is near universally referenced as a corruption-prone area for public officials (Dimant & Tosato, 2018). By highlighting the universality of this pattern around the world, this research demonstrates that it is better viewed as a system of procurement is regulated opportunity than something defined by culture or governance failure. Crucially, the consequences of corruption in procurement are far-reaching, extending well beyond wasted resources. It diminishes institutional efficacy, disrupts the dynamics of competitive markets, and excludes legitimate firms from the bidding process. In their research

on the phenomenon of corruption in the American context, Dincer and Johnston (2025) disclose a decline in civic participation caused by corruption linked to procurement, and some local development programs result in a distortion of civic priorities and ultimately yield a perception of systemic injustice. The impacts of these much greater in jurisdictions that have anti-corruption frameworks, including legislation about procurement, but do not consistently follow or enforce those regulations, as it creates a legal veil of collusion and favoritism. Aspects of the social degree are no less extreme. Adesola et al. (2024) characterize corruption as a pandemic, given its significant acceptance and penetration into the public's expectations, erosion of ethical boundaries, and a general sense of resignation in citizens when public tenders and infrastructure contracts are seen as a foregone conclusion and/or manipulated process. Institutionalization of bribery and fraud in procurement, normalized and seen as acceptable, overwhelms legitimate transparency initiatives such as open tender platforms, integrity pacts, and even assertive community engagement. Elliott (1998) warned, at a time when globalization was in its infancy, that the growing complexity of international trade and overseas aid flows would create growing opportunities for procurement corruption, unless accountability was supported by robust enforceable oversight mechanisms. Elliott's observations are prudent today in increasingly cross-border contracting and digital procurement contexts that support corruption at the national or transnational level.

What remains constant is not a failure of institutions, but a maintained structural imbalance between legal formality and political practice. The presence of anti-corruption laws and procurement guidelines is often meaningless if they are not enforced; or the oversight mechanisms lack independence while ethical practices are displaced by patronage networks. Muhammad, Wasiu, and Ahmad (2023) note that in multiple African nations, corruption in procurement exists not only due to the absence of regulations; it exists when favoritism is a preconceived mechanism of access to opportunity and fraud is tacitly accepted. This situation reflects a larger global problem wherein formal reforms to procurement practices have not become institutionalized and accepted when in direct competition with informal norms and elite capture.

Importantly, structural realities are not limited to Global South contexts. In high-income nations, procurement-based corrupt practices provide evidence of illicit practices that are adaptable, and that exploit the complexity of the system. As Grandes & Coremberg (2020) note, corruption in procurement works in "accounting shadows" where "misreporting," "overpricing," and "diverting funds" (p. 378) are possible in budgets, auditing, procurement and, ultimately, without immediate detection. Accounting shadows are not a fortuitous administrative fault; they are products of a broken and fragmented governing apparatus, in combination with a rapid digitalization of state apparatus and lack of inter and intra-agency coordination. When these accounting shadows exist alongside the imperative for public contracts with high stakes, they create a consistent yet subdued erosion of institutional integrity. The repercussions of such systemic erosion are both economic and civic. Mo (2001) found, empirically, that corruption has a negative effect on investment and economic growth, especially in sectors with large public infrastructure. Akçay (2006) underscores this link with human development—specifically the inability to advance health, education, and

housing when procurement is not sufficiently binding and public good at the core of programming delivery. These failures have a commonality, which is a manipulation of decision making towards those connected in contrast to the public good. Awarding procurement contracts to the politically favored and not the qualified reduces efficiency, quality and advancement of development over the long term.

The effect on the social sphere due to procurement corruption is equally concerning. Myint (2000) portrays corruption as recasting the expectation for the public, leading on to cynicism and disengagement. Citizens assimilate the belief that influence, connections, and payment are more important than legality, merit, and transparency. While well-intentioned efforts to inject transparency take place, regardless of the seriousness of the agenda, any processes or functions characterized as procurement will often fall into disrepute regarding their integrity, simply due to the past perception of corruption. Bălan-Liseanu (2023) goes even farther than this in worrying about how the application of corrupt procurement becomes a threat to human security – when public resources are used in service of narrow interests and leaving social needs unmet. In spaces where roads are left undone, hospital equipment is comprised, and housing projects are suspended due to the corruption of collusion and fraud the abstraction of corruption evaporates and, in its stead, enters every day visible ruptures to social contract.

These failures are much an issue of the tools of measurement as well. As noted by Franzoni (2025), the risk in a context of unmeasured procurement corruption is that the traditional constructs of corruption would likely fail to detect tenders' collusion, invoice fraud, or the use of shell companies. The invisibleness of procurement remains and difficulties in interpreting and solving procurement corruption remains as a consequence. Traditional corruption rankings may provide an understanding of aggregate perceptions but rarely serve to understand the descriptive mechanics of legal, practical, or technical procurement corruption prominence.

The complexities of procurement space are often a breeding ground for corruption obscurity. Procurement fraud will not always be glared at in some blatantly illegal manner suggestive of policing. Often it is elusive and exists in 'grey area' of a policy interpretation, selective targeting for relative enforcement, discretion of politically directed appropriateness or ambiguity noncompliance. Graycar and Sidebottom (2012) stress, the longest standing, continuous and persistent forms of corruption will be the corruption most difficult to observe using traditional oversight: no bid pre-ordinances, collusion with suppliers, and weighting technical specifications toward eliminating competitors that are not favored. But these acts are not anomalies and are reoccurring patterns engendered by systemic and rooting flaws in institutional design and asymmetries of knowledge between officials, bidders and the public. The analysis of corruption within the local political economy of procurement unveils a more profound issue, wherein public contracting decisions are too often made based upon the influence within the policy networks and less so on the merits of the policy. Elliott (1998) observed at the crux of trade and public finance warned that globalization platform would not eliminate corruption but reshape it in favor of a new structure to engage it—as part of establishing cross-border transactions, privatization, and funding

from international development. He was right, and procurement-related scandals increasingly include international firms, offshore accounts and transnational legal arbitrage. However, all this is not new, and it is for the most part, the same corrupt action that has simply changed from—the diversion of public resources for private or political gain, sometimes under the cloak of lawful processes.

This issue of the erosion of integrity in public procurement, however, is much broader than a bureaucratic topic—it is a democratic topic. As Dincer and Johnston (2025) argue in regard to the U.S. context, corruption in public procurement processes threatens public accountability, skews electoral incentives, and undermines the legitimacy of regulatory institutions. When public procurement becomes the method of rewarding loyalty, or funding political instruments, then the procurement system is seized—more than economically but also institutionally. Public distrust, faith, and support diminishes when the public infrastructure and public services are unraveled and flawed, not completed, or abandoned, and when the public senses that public procurement decisions are made behind closed doors. Corresponding efforts to countering corruption in procurement are continually undermined by the very systems that are designed to end corruption in procurement. Although many jurisdictions have oversight agencies, anti-corruption commissions, and auditing institutions to enhance accountability, several of such institutions will often only function within certain limits for multiple reasons, which may include political interference, lack of adequately sustainable funds, and lacking required capacities or technical expertise. Ahmadjonov (2025) argues that this paradox can be found in public administration and describes the very institutions charged with integrity, are often the institutions most susceptible to being manipulated. Instead of offering openness and impartiality through legal, rules-based, and procedure-driven systems, procurement becomes a battleground for negotiating value and navigating around legal procedures, through whichever means available, while offering cover for favoritism and dishonesty.

The sticking power of corruption in procurement, some thirty years after the first rule-based systems offered anticipation to stop and curb corruption raises some questions regarding how we design anti-corruption and accountability systems moving forward. The issue is not simply a lack of laws or procedures, but there is often a misalignment between formal structures, such as rules for procurement, and informal power relations. Annisa and Lavides (2025) show this in the Indonesian context, by arguing that even the most “internationally compliant” or “technically comparable” procurement systems will perform poorly in high political interference and/or in weak institutional trust. The result is a putative legally functioning system but one which practices discretion is a system where procurement appears rule-based with all the legitimacy of rules-based procurement, but is often a negotiated exercise of power. The endurance and flexibility of corruption in public procurement indicates that traditional approaches, while necessary, simply do not go far enough. Though formal laws, procedural audits, and compliance systems are useful, they can always be circumvented in systems of governance marked by the three characteristics of obscurity, discretion, and political patronage. As Rose-Ackerman (2005) and Enste and Heldman

(2018) show, anti-corruption initiatives founded solely in either legal formalism or administrative reform struggle with the structural asymmetries of information, power, and accountability to prevent procurement manipulation. The end result is a jaw of a cycle, of reform but no reform: periodic scandals followed by new oversight and controls that are gradually absorbed or bypassed by the very systems of governance being repaired.

Breaking the cycle of no reform requires more than conventional institutional repairs. It requires structural innovations in the form of transparency, confidence into accountability, and to address discretion; the very flashpoint of favoritism and collusion. In this light, the possibilities for technological solutions; especially for digital integrity tools, distributed ledgers, and smart contracting mechanisms have emerged and started to gained ground on the global stage. As Franzoni (2025) argues, to focus on only measurement and subsequent enforcement, and to make the goal of anti-corruption initiatives, the future of such initiatives will consist ameliorating the architecture of governance to make corruption technically complicated and economically irrational.

Nowhere is this more urgently needed than systems of public procurement; where corruption is not simply an issue of economic inefficiency, it undermines citizen trust in the state. Public procurement is the 'gate marker' between power of the state and access to the market: between the use of tax-based public resources and the delivery of service by the private sector. Once corruption introduces this interface, the implications are far greater than an inability to adequately provide a public good with respect to the budget: it deprives the rule of law of credibility, impacts the efficacy of the delivery of public services, and undermines the legitimacy of democratic governance (Bălan-Liseanu, 2023; Muhammad et al., 2023). The objective then is not simply to identify and police the scope of symptoms of procurement corruption, but to rethink and redesign the system of procurement in a manner that limits discretion, allows for traceability of transactions and creates confidence into the processes of oversight from beginning to end. The characteristics of blockchain technology—factors such as immutability, transparency, decentralization, and programmability—offer one avenue of systemic change. Its power is real to disrupt procedural ambiguity and informational asymmetry that has historically enabled procurement corruption to flourish. However, achieving such systemic change requires much more than technological utopianism. It requires an empirical understanding of the functional relationship between blockchain, legal norms, regulatory environments, and institutional contexts across jurisdictions.

This dissertation meets that challenge, by focusing on public procurement in three democratic systems—Italy, Canada, and the United States—this dissertation analyzes ways that the technology of blockchain could be effectively used as a meaningful legal-regulatory intervention to address the systemic roots of corruption—rather than merely as a technology for technology's sake. In doing so, it goes beyond the lofty potential of transparency and explores specific governance

circumstances under which blockchain could support anti-corruption efforts in public procurement systems.

1.1.2. Limitations of Traditional Anti-Corruption Measures

Despite many global attempts to reform public procurement systems for decades, traditional anti-corruption approaches rooted in legal and institutional frameworks have historically not been successful at drastically eliminating corruption from these systems. While legal and institutional frameworks provide the fundamental structures to build upon them, studies have called attention to several structural vulnerabilities of these frameworks, including excessive reliance and utilization of rules, limited capacities for enforcement, excessive political intrusion or interferences in decision making, and inability to deal with the adaptive and opaque forms corruption takes in real public systems (Persson, Rothstein, & Teorell, 2013; Marquette & Peiffer, 2018). The primary conceptual framework, which utilized the theory of principal -agent approach to explain corruption and corruption systems, misrepresents systemic corruption as agent misbehavior and had limited focus of issues of collective action problems, embedded networks, and political incentives that maintain patronage systems and corruption (Persson, Rothstein, and Teorell, 2013; Marquette and Peiffer, 2018). Traditional methods of legal and institutional approaches can fail us through ambiguity, institutional opacity, and limited considerations surrounding oversight, along with the elasticity of corrupt networks as reasons for limited reform and constrained reform of public integrity systems, which are complicated and hardly managed through oversimplified compliance (Gray, 2021). After decades of reforming public procurement systems, strong formal reforms continue yielding no genuine results, and demand the development of approaches that are more context-sensitive, transparent and systems-integrated. The subsequent section will discuss these constraints through a theoretical, institutional, procedural and behavioral lenses. While anti-corruption efforts abound as strategies have spread rapidly in the last thirty years, corruption continues to flourish in public sector systems as a whole and in public procurement, in particular, due to the nature of this context: public procurement (a process, system, domain) is often: opaque, discretionary, and high value. Legal and institutional frameworks, accepted in general as constitutive of good governance, dilute characteristics of action and institutional vulnerability that are sometimes obscured. Although as Heeks and Mathisen (2012) described shared the action of superfluous transmissible best-practice models adopted with disregard to institutional context; however, these disconnects lead to breakdown breakdowns in enforcement and legitimacy. This then becomes especially burdensome to practitioners in jurisdictions, when an institutional legal framework may look strong on paper, it does not appear to be connected to enforcement or political will. A central limitation of many anti-corruption regimes lies in their reliance on a legalistic approach that assumes rational compliance with rules. However, as Persson, Rothstein, and Teorell (2013) contend, systemic corruption cannot be dismantled through individual sanctions alone

when corrupt behavior is embedded in collective norms and expectations. The view that corruption is a principal–agent problem has, in many cases, mischaracterized its actual functioning as a collective action dilemma—where the incentives for individuals to act cleanly are weak unless they can trust that others will do the same. This insight is critical for understanding the limited efficacy of traditional approaches, especially in environments where public officials operate within entrenched informal networks that reward non-compliance.

Moreover, traditional anti-corruption measures are often undermined by bureaucratic discretion and lack of transparency in decision-making processes. Smart (2018) highlights the "unbearable discretion" of street-level bureaucrats, whose interpretive autonomy in implementing policies creates opportunities for selective enforcement and favoritism. This discretionary space becomes a fertile ground for corruption when combined with institutional weaknesses such as inadequate oversight, limited citizen recourse, or political interference. Similarly, Gillespie (2021) emphasizes the difficulty of mounting an effective public interest response to corruption orchestrated by the state itself—where accountability institutions may be complicit or structurally powerless.

The failure of conventional legal tools is also evident in international and transnational anti-corruption efforts. As Kruessmann (2021) notes, transnational anti-corruption law often suffers from normative overreach and lacks binding enforcement mechanisms, resulting in rhetorical commitments with little practical effect. This problem is mirrored in domestic systems that formally adhere to international standards such as the United Nations Convention Against Corruption (UNCAC) but exhibit persistent impunity and elite capture in practice. Legal alignment, in this sense, becomes more symbolic than transformative.

The proliferation of trust deficits further weakens the efficacy of traditional anti-corruption institutions and statutes. Adelopo and Rufai (2018) describe the skepticism of citizens toward anticorruption institutions in the context of historically failed ant-corruption institution, thus dissuading civic participation and compliance. Mistrust of such body or statute is not without its basis; where anticorruption statutes are selectively ignored or weaponized politically, the anticorruption body in question is in reality perceived as a legitimacy mechanism, as opposed to a reforming authority. Marquette and Peiffer (2018) assert that any serious anti-corruption initiative must deal with the “real politics” of power, networks and incentives, neither of which are accounted for adequately in the paradigm of traditional legal-institutional understanding of law.

Beyond the structural limitation of accountability mechanisms and institutional deficit, the operationalization of anticorruption authorities as have had been designed is beset with repetitive internal inconsistencies or operational fragmentation. Batory (2012), speaking about Central and Eastern Europe observes that anticorruption laws are typically created without sufficient proxies, mechanisms, or incentivization leading to ambient frustration in implementation or lax commitment and policy fatigue. Statutory obligations and legal rights are not in synchrony with multiplier effects of institutional planning, often leading to create anticorruption bodies that are

awkwardly understaffed and often politically stifled, engendering underperformance or co-optation, and eventually return to status quo. As a result of the lack of disaggregation, legal statutes often more resemble bureaucratic procedural ritual than agents of reforming change. The policy-practice gap between design and impact wronging occupies what would otherwise be a marginal space; yet this gap is the cauldron of systemic ineffectiveness. This issue is similar to Gray (2021) who illustrates how corruption develops in procurement systems even though these are subject to formal oversight institutions. South Africa provides the example of entrenched collusion between public sector officials and private sector contractors that run parallel to the formal procurement system and essentially circumventing rule of law controls. These collusions are not just aberrations of formal procurement processes but alternative governance arrangements that exploit loopholes, delays and ambiguity of regulation stress formal institutional traditions. Other jurisdictions face similar or different variation of stymied anti-corruption accountability measures, but differ on institutional entrenchment and measures of transparency and safety nets.

In such regimes, legal enforcement mechanisms often prescribe generalist frameworks to corruption that contract to establish principles and legal situations for deliverables and ultimately limit enforcement relevance. The claims of Sotola and Pillay (2022) suggest that anti-corruptions plans are often evidenced as 'thin' because their theories are lofty but their practice becomes obscured by the lack of reflexivity to understand the everyday practice and thinking like thieves and street victimization mandates an ontological assumption of otherwise of the public procurement operational services. The thinking and theory are being overly generalist, producing imprecise interventions legally for not all practitioners are corrupt or acting in deliberate subject matter, so legitimate practices go punished when public procurement contexts muddle high complex processes and cluster multiple institutional actors. The absence of applicable learning to understand anti-corruption complete proxies remit accountability and creates systemic risk liability systems as risks are hidden by false institutions.

Feikema (2024) describes a potentially deeper set of dilemmas philosophically believed to complexify anti-corruption law as a legal fiction more intentional than guiding a practice. The falsehoods of regulatory control can even play to perfection and legitimize the very institutions that have permitted endless malfeasance history being contextualized. The performative value of law only worsens public trust like suggested above that will flourish only when this future is always destined and framed on the temporary as institutions are normalized. mathcing with wider transformative practices and broader structures.

Then there is the actual weaponization of ostensibly legality to act as camouflage for informal abuses witnessed in gaslit modes for no rural reform or maturity only produced what some scholars termed as 'legalized corruption.' There is also a central vulnerability of traditional anti-corruption initiatives: an ignorance of human and institutional psychology. Smart (2018) and Meza & Pérez-Chiqués (2020) raise our awareness of evidence that behavioral patterns, social ties and localized incentives are often more important than legal obligation. Street-level bureaucrats, purchasing officers and local officials can do their work in formal and rule governed ways, while also taking

part in informal behaviors governed by social norms of obligation, including personal gain, survival and in-group loyalty. These realities represent some understanding of why anti-corruption regimes' focus on rules and codified proscriptions, have a difficult time cutting past the informal structures that govern actual behavior. The nature of embedded behavioral patterns mean that enforcement outcomes have often been inconsistent, and highly conditional, reflecting what Gillespie (2021) refers to as a "credibility trap;" an organizational configuration in which anti-corruption agencies and frameworks show all signs of functioning, yet are bound by adjudicating logic, making them structurally incapable of exercising power.

This separation of formal and informal norms has also been identified in international development situations. For World Bank projects aimed at governance and anti-corruption, Kuipers (2021) notes that anti-corruption strategies driven by donors prioritize legal integration and compliance rather than institutional readiness or political viability. While donor-led governance reforms will usually be constructed using globally acceptable best practices, they are rarely situated in the realities of the systems that the rules are meant to govern. This disconnection leads to failed implementation of superficial reforms that had little chance of impacting deep institutional change. When these externally-derived rules enter systems that are already missing key elements of legitimacy, trust or transparency, they risk adding to cynicism and disengagement rather than compliance and accountability. Corruption is not merely an institutional concern; it is also an epistemic one: What is corruption and who says? Marquette and Peiffer (2018) emphasize the importance of understanding that diverse actors ,officials, citizens, donors, and businesses conceive of the notion of corruption qualitatively differently. They may criminalize certain behaviors through legal definitions, but the underlying social mechanisms, which may harm even more (but are socially normalized), are ignored. Here, anti-corruption law may lack conceptual nimbleness to address context-specific manifestations of abuse, especially in sectors like procurement, where informal negotiation, clientelism, and discretionary allocation are typical but exceptionally difficult to pursue. Traditional approaches generally globalize the concept of corruption through legal typologies that cloud the clear representation of the complex actualities of systematic misconduct.

Kruessmann (2021) further demonstrates the failure of legalistic approaches, particularly at the transnational level, suggesting that anti-corruption law is neither coherent nor enforceable in substantive ways. The dissemination of norms across jurisdictions—largely driven by multilateral institutions and international conventions—does not lead to a significant level of enforceability or harmonization. Typically, such norms lead to a convergence of legal injunctions without engaging with operational clarity, and allow for states to performatively advance further commitments without inquiring into the established or replicated systems of power. That is to say, these institutions carry normative weight and further widen the schism between law and politics, diminishing public trust and collective accountability.

Moreover, even high-capacity states like those in North America and Western Europe use traditional legal mechanisms to similarly address corruption deeply embedded in procurement. Gray (2021) provides clear evidence that regulatory regimes may look strong on their face while

being undermined through collusion among insiders, strategic temporizing, and/or agents who exploit subcontracts to extract rents. In these instances, corruption is not merely a matter of rule violation, it is a matter of pervasive governance architectures allowing actors to perform in legislative gray zones. When anti-corruption law does not acknowledge the complexities of governance, it not only fails to be an effective substantive remedy but may provide the necessary basis for actors to better exploit procedural legitimacy for more complex forms of manipulation.

The capability of corruption to persist unimpeded by reasonably impressive sets of legal deterrents also embodies a failure of many anti-corruption frameworks to respond to institutional feedback or adapt to changing risk environments. Batory (2012) described a number of cases in Central and Eastern European countries that had legislated and pushed forward anti-corruption institutions with static mandates that simply did not develop in step with emerging forms of procurement fraud and digital vulnerabilities. As a result of this inertia, these types of institutions tend to be less proactive and merely reactive, not least in areas where corruption usually manifests through contract designs becoming more complex with regard to rules of enforceability, all while also involving intra-border movement of funds. The result is a situation whereby the legal instruments diverge from the dynamic relational practices that they are intended to govern, as described by Owusu, Chan, and Hosseini (2020), whereby a degree of correlational asymmetry in implementation emerges in the realm of infrastructure procurement, albeit with an even higher incidence of corruption associated with the misalignment of enforcement incentives and fragmented oversight in favor of elite interests.

Another impediment concerns the institutional separation anti-corruption agencies. For example, Quah (2021) analyzed several Asian states and set out different instances of the working of anti-corruption bodies existent without enough insulation from the political process. It does not matter at times whether investigative mandates were enshrined as part of law, as absent any functional independence, secured (longer) terms for staff, or protections from dismissal actions for political purposes severely compromise the institutions operational credibility. With those contexts lacking those exclusions, anti-corruption bodies must either enforce selectively, or deliberately clear anti-corruption investigations, both actions which may do little to offset elite dissipating authority. This is not exclusive to authoritarian systems, either; a democratic backdrop does not exempt anti-corruption instruments from politicization in nature, either through over-reliance on discretionary budgets, or appointments processes for judicial systems, or even political maneuvers in legislatures.

Then, given the brute force at which anti-corruption campaigns are employed as political legitimatizing processes, Adelopo and Rufai (2018), completed an exhaustive analysis of the ramifications in elite-dominated contexts that face long historical antagonism yet deep in situ trust-deficient atmospheres. In such hostile environments, instead of abandoning anti-corruption frameworks as a discrete agenda, they can be manipulated actively as means of delayed political legitimacy, whose consequences are preserved by institutions that purportedly defend the rule of law. Through this kind of politics, the legitimate role of the civil society is cohesive and further

facilitated through the nature of exclusions, and self-feeding distrust in public institutions, increasing in degree over time, which of course erodes trust in public institutions to begin with. In addition to this, there is an increasing acknowledgment that conventional approaches to anti-corruption are usually framed in terms of a linear rationality of reform: changing the legal environment leads to change in institutions, which in turn leads to compliant behavior. However, as indicated by Persson et al (2013) and Marquette and Peiffer (2018), this is problematic because it ignores the informal norms and social logics behind much of public procurement behavior. Legal change in the midst of a context of systemic corruption without a change in norms can yield unintended consequences, such as strategic behavioral adjustments by corrupt actors, a failure to obey the rules, or the displacement (not eradication) of corruption (Dávid-Barrett and Fazekas, 2020). When procurement officers or suppliers believe others are still engaging in corrupt behavior, the disincentive to behave honestly erodes, regardless of the new or more severe rules in place.

These limitations demonstrate the need to re-examine the epistemological and structural assumptions that underlie traditional anti-corruption approaches. Indeed, as noted by Feikema (2024) and Kuipers (2021), the present context requires not just a consideration of formalistic rule-making in anti-corruption but, instead, it is time to embrace strategies that engage with underlying institutional incentives, sectoral complexities, and behavioral features that shape corrupt behavior. Legal and regulatory frameworks cannot be abandoned as a solution to corruption; however, their effectiveness does not depend on textual specificity or territorial synchronicity alone. They depend on adaptation to context, credible threats of enforcement, and trusted public institutions - this is an aspect often neglected, or assumed away, in our traditional conceptualization of corruption.

An all-encompassing investigation into established anti-corruption strategies must also acknowledge the symbolic function of many of the legal reforms. Feikema (2024) elaborates that legal establishments represent an illusion of control in the stylization of anti-corruption regulations and rules, disguising more profound institutional inertia which impedes any real change. Such an illusion is carried through periodic reforms and commissions, many of which are not substantive. Where procurement corruption is the norm, as seen in parts of Southern and Eastern Europe, this pattern can lead to what Smart (2018) calls "institutionalized discretion," where the law exists, but law is enforced through informal hierarchies, personal ties or the convenience of politics. Therefore, the existence of an anti-corruption law may offer international legitimacy and/or donor approval, rather than evidence of any real or measurable integrity.

The structural complexity of public procurement systems has raised other challenges for traditional compliance models. Gray (2021) and Dávid-Barrett & Fazekas (2020) both note how procurement networks—comprised of political actors, bureaucratic officials, private provision suppliers, and intermediaries—are often locked in opaque chains of transactions that are difficult to follow via audits. Even though e-procurement systems and transparency tools are implemented, actors

involved in corruption will craft collusion, front companies or bid-rigged schemes to take advantage of loopholes embedded in the system. In these experiences, typical monitoring tools will be thwarted by the ingenuity of actors who have deep local knowledge of the complexity of these systems, and typically some level of political protection. Therefore, traditional measures, which tend to focus on the language of documentation or procedural compliance are not responsive to the increasingly networked and adaptive character of corruption.

Another recurring limitation is the under-utilization of public accountability mechanisms. While there has been much discussion and focus on legal and administrative control, there has been a relative neglect of the institutional capacity for the participatory dimension of anti-corruption. As Gillespie (2021) and Kuipers & Verhey (2023) have suggested, anti-corruption is much more effective if there are other spaces devoted to citizen monitoring, whistleblower protection, and civic audit. Yet, many laws do not allow for such participation because of technical words, information access, and/or procedure. This creates an insulation from technocracy, which undermines the ability to hold processes to democratic accountability, and is also elitist, bounded, and closed. In turn, as one would expect, this interjects distrust and disengagement from citizens in the anti-corruption process, which amplifies the trust deficit in state institutions.

Finally, the lack of corruption in otherwise legally advanced systems still indicates that legal frameworks, while necessary, are not sufficient. Rothstein (2021), explains that checks on corruption require a broader governance reform that unravels the bureaucratic incentives that allows for unethical behavior, reintroduces trust and institutionalize impartiality. Change in law requires change in clear enforcement, political will and structural realignment at multiples levels of administration. The very nature of attention about procurement corruption in both developing and developed contexts indicate that unless those conditions precede scandals, anti-corruption legislation will erode, circumvented, and at worst, co-opted. Therefore, traditional models need to change-not by abandoning legality, but embedding legal frameworks within a more adaptive, transparent, and participatory system of governance.

Given these constraints, this dissertation contends that blockchain technologies, while not likely to overcome these entrenched biases, leverage inherent traits of immutability, transparency, and decentralized verification, which could provide a significant disruption to these institutional flaws. Furthermore, these technologies will only be effective with some form of legal and institutional ecosystem surrounding them. The next chapters will outline how blockchain may function to support—not supplant—traditional forms of securing trustworthiness and accountability by embedding them in the system. This dissertation will study that intersection comparatively, looking at public procurement systems in Italy, Canada, and the United States that exhibit legal sophistication while still being vulnerable, but where new technologies could provide the impetus for institutional change.

1.1.3. The Advent of Blockchain Technology

Blockchain has emerged in the past few years as an important new disruptive technological paradigm able to innovate not only financial mechanisms but also public governance, law and procurement. Blockchain technology was initially designed as a supporting infrastructure for Bitcoin (Nakamoto, 2008), and has emerged as a multi-functional and decentralized system containing four defining characteristics: decentralization, immutability, transparency, and auditability. These features, which are derived from cryptographic design and consensus verification, allow blockchain to function as a "trustless," tamper-proof digital ledger: a ledger, while not limited to cryptocurrency (Zheng et al., 2017; Yaga et al., 2018).

Decentralization is the characteristic that distinguishes blockchain from traditional databases. Instead of relying on a centralized authority to verify and preserve the integrity of the data provided in the system, blockchain allows for validation and storage of ledger copies to occur across multiple nodes independently (Monrat et al., 2019). The resulting network of decentralized consensus ensures the ledger can be operationally resilient with regard to single points of failure and tampering. Only transactions that have been validated by a majority of nodes in the web will be encoded into the ledger, with the majority of browsers relying on a protocol of consensus to achieve including Proof of Work, Proof of Stake and Practical Byzantine Fault Tolerance (Bhutta et al., 2021) as examples. Once a transaction is validated and encoded into the ledger, it becomes virtually impossible to alter, creating a permanent chronological chain of records that your last entry exists.

Immutability is the feature enabled by cryptographic hashing by linking one block to the previous block creating a chain that is designed to mathematically prevent tampering (Dong et al., 2023). Attempting to change the transaction would require recomputing all the other associated blocks while being validated by the majority of the nodes. The complexity associated with performing that level of computing makes this completely impractical. A further enhancement to the immutability of a transaction record when encoded is the use of Merkle trees. The use of Merkle trees is the aggregation of hashes in each block aggregated into a single hash (root), verified as secure and efficient for validation when dealing with larger datasets (Chowdhury et al., 2019).

The characteristics of transparency and auditability are predicated upon the fact that blockchain is a public ledger, especially in the case of permissionless systems like Bitcoin and Ethereum, all participants can see the status of the ledger and trace the history of any transaction back to the original transaction, thereby creating a tamper-proof audit trail. These features make blockchain attractive to sectors that need accountability and traceability, such as financial audits, compliance with regulations, and public procurement (Pilkington, 2015). Even in permissioned or consortium blockchains, where access is limited to specific members, the underlying structure maintains verifiability of records and consistent transaction histories among trusted parties (Frizzo-Barker et al., 2020).

The unification of these core features—decentralization, immutability, transparency, and auditability—position blockchain as a significant infrastructure for digital trust in open and semi-trusted environments. Although designed to enable the exchange of peer-to-peer currency, blockchain technology has been recognized as a versatile tool that allows for tamper-proof records, automated processes through smart contracts, and increased trust of digital systems. These features have led to worldwide interest in using blockchain technology to redesign public systems, especially in sectors susceptible to corruption or inefficiencies.

The architecture of blockchain technology is grounded in cryptographic principles that ensure the integrity of data, secure identity verification of participants, and immutable transaction logging and history. Fundamentally, blockchain technology relies on widely used public key cryptography, digital signatures, in addition to cryptographic hash functions for record retention and accountability without a centralized authority (Centobelli et al., 2021). Public key encryption allows participants to sign transactions with their private key and allow a single public key to identify the participant while any third-party user confirms the signatory of the transaction is authentic. This type of cryptographic signature provides guarantees of non-repudiation and authenticity while allowing participants to engage in secure transactions without revealing personal identifiable information that can be used for financial or administrative transaction purposes (Rahmani, 2022).

Digital signatures are a critical component of trust in blockchain systems. In systems such as the Bitcoin and Ethereum networks, each transaction in made through the use of a digital signature based on the sender's private key and verified through the sender's public key. This makes it difficult for unauthorized actors to create valid transactions. These mechanisms are of importance to public procurement process such as contract enforcement/ compliance and fraud detection, where you require digital traceability and non-repudiation to hold people accountable. The same is true of hash functions like SHA-265 used in Bitcoin, to produce a unique, non-reversible representation of transactional data, based on its data structure, for block creation and validation. Any change in input creates a new hash function and lessens the previous data state. Because of this a single bit change (the change of a block/ record) is sufficient for us to detect unauthorized changes (Guo, 2022).

The introduction of smart contracts only strengthens the disruptive power of blockchain technology. Smart contracts—most often popularized in public discussion by Ethereum—are codes with rules and conditions programmed to self-execute, automatically enforcing a contract between parties on a blockchain platform (Hewa et al., 2021). Smart contracts eliminate reliance upon third parties and they also have the potential to eliminate potential human errors or human manipulation. The first clear use of smart contracts in public systems could be into procurement workflows, automatically controlling procurement with secured bidding rules and payment on verified milestones, each milestone can be downloaded from the procurement ledger transparently. The behaviors defined by the smart contract were executed automatically by the smart contract—

done in a manner that guaranteed procedural fairness—simultaneously each milestone execution was validated by the ledger's immutability.

Furthermore, consensus mechanisms merit discussion because of their importance in the establishment of distributed trust. A consensus mechanism—like Proof of Work, Proof of Stake, or Delegated Proof of Stake —enables distributed nodes to arrive at an agreement regarding the current state of the ledger without delegation to a trusted party or central authority (Hafid et al., 2020). Accordingly, there are trade-offs between energy efficiency, scalability, and an attack vector during the process of choosing consensus in attending to the important goal of designing secure and useful blockchain systems. In particular, many public blockchains like Bitcoin and Etherium have utilized PoW mechanisms for reasons of a high level of security, despite P0W being resource intensive as compared to other mechanisms without a proven track record. Interestingly, enterprise- or government-oriented platforms such as Hyperledger Fabric utilize faster consensus models like Practical Byzantine Fault-Tolerance (PBFT), more conducive to the sector's demand for control, access, and comparatively lower energy expenditures due to energy cost incentives (Krichen et al., 2022).

The aforementioned digital methods - cryptography, smart contracts, and consensus algorithms - are not only novel advances in computation; they are the indispensable cornerstones of a technology that will alter accountability systems. In areas that can suffer from deep inefficiencies and institutional corruption, and where the systemic risk and cost of corruption are the highest such as public procurement, blockchain can deliver procedural certainty, immutable records, and decentralized validation that will reconfigure relationships of power and enhance institutional integrity. Consequently, blockchain does not embody a technical revolution; it is a systemic revolution and is based on a logic of digital trust.

The historical perspective of blockchain technology reveals a clear evolution from a specific embodiment in the Bitcoin protocol to a generalized and multi-functional infrastructure facilitating the free and open exchange of information and value within decentralized systems. The historical perspective of blockchain technology captures the continuing technical developments, but more especially illustrates the evolving and varying concepts of trust and verification in digital spaces. An early formalization of a blockchain-type architecture was proposed by David Chaum in his cryptographic protocols in 1982, and further developed in 1991 by Haber and Stornetta who described a process to securely timestamp digital documents (Guo & Yu, 2022). The breakthrough occurred in 2008 with the emergence of Satoshi Nakamoto's Bitcoin whitepaper which presented a fully-fledged blockchain system that challenged traditional payments systems and introduced a peer-to-peer, electronic cash system with no trusted third party.

The significant achievement of Nakamoto was to incorporate pre-existing techniques in cryptography with a distributed consensus mechanism known as Proof of Work (PoW), which permitted secure and decentralized validation of transactions. In this manner, blockchain allowed a very old problem in distributed computing, namely achieving consensus in a trustless

environment, to be resolved. Bitcoin was started in 2009 as the first operational cryptocurrency, and the first practical use case of blockchain. For every block in its chain, Bitcoin was designed to include a reference to the preceding block using a cryptographic hash. Therefore, each block would ultimately form a verifiable and immutable sequence of records over time. The chaining of blocks and consensus established a fundamental foundation for other blockchain platforms (Zheng et al., 2017).

The move from Bitcoin to Ethereum was arguably the most significant evolution in both the technology and thinking around blockchain. Proposed in 2013 by Vitalik Buterin and introduced in 2015, Ethereum changed the blockchain ecosystem in several different ways. First, Ethereum added ways to develop decentralized applications and smart contracts on the blockchain by using a Turing-complete scripting language. Thus, Ethereum added programming capabilities to blockchain technology (Lin et al., 2024). For these reasons, we refer to Ethereum as Blockchain 2.0, which introduced a move towards programmable and multipurpose distributed systems. Ethereum's inventiveness inspired new decentralized applications in all areas of society - especially in governance, identity, and automated compliance and decision-making. As will be described in more detail in the next chapter, Ethereum reframes our understanding of how blockchain technology can disrupt institutional processes in both the public and private sector.

Alongside the growth and rise of Ethereum, blockchain technology for enterprise-grade applications has become apparent. The Hyperledger project, started in the Linux Foundation in 2015, is one such example. Unlike public blockchains, Hyperledger frameworks, including Fabric, Besu, and Sawtooth, are designed for environments where participants are known and vetted, or permissioned environments. Hyperledger frameworks prioritize scalability, privacy, and compliance with regulatory requirements—all key features of applications in areas like public procurement, healthcare, and supply chains. Hyperledger consensus algorithms have also been engineered for low-latency environments and are well-suited for their use in environments where energy efficiency, fast finality, and control of the governance (Patil & Bhosale, 2023) is key. These are important developments recognizing that blockchain is not an afterthought, but flexible to various operational, pragmatic, legal, and technological specifications in relation to the practices being digitized.

With the maturation of blockchain, researchers and developers began exploring application scenarios across multiple sectors. Rather than financial transaction-based scenarios, the immutability and transparency features of blockchain created a viable technology to solve problems involving record-keeping, auditing, and preventing fraud. Research and applications in many sectors emerged for example healthcare as managing patient records, logistics as improving traceability of supply chains and legal as create and manage digital contracts and notarization. Notably, the intersection of blockchain’s technical affordances and the normative aspects of public sector governance—transparency, accountability, traceability—has stimulated growing interest in its use for anti-corruption applications. The development of applications in diverse domains signifies that blockchain is not solely a cryptographic technology, but could act as a governance

technology with systemic implications for how institutions manage information, enforce rules, and develop trust with the public.

1.1.4. Potential of Blockchain for Governance: Improving Public Sector Integrity and Efficiency

Over the past few years, the rapid increase in the overall uptake of blockchain technology has indicated the possibility of a transformational change in the way that governments think about, deliver, and evaluate public services. Originally developed as part of the decentralized finance movement, blockchain has matured into a broadly applicable governance architecture that has the potential to address long term efficiency, transparency, and corruption challenges at the public sector organizational level (Bustamante et al., 2022; Kassen, 2022; Ibrahimy et al., 2023). As governments face growing levels of public distrust, fiscal pressures for accountability, and demands for transparency, blockchain has the potential to be not only a technological innovation but also an institutional logic based in immutability, automation, and decentralization which aligns with good governance principles.

Blockchain is essentially a distributed ledger that records an immutable list of time-stamped data, verified via consensus (Cagigas et al., 2021). The cryptographic guarantees provided by blockchain would address one of the most debilitating weaknesses of public administration—data integrity—by reducing opportunities for tampering. Centralized databases rely on faith in the institution with ultimate control, while blockchain achieves "trustless trust"—meaning transparency and trust emerge from design features of a set of protocols, not an institution's reputation (Batubara et al., 2018; Ibrahimy et al., 2023). This trust is especially important for organizations with possibilities for corruption or manipulation over process, especially in areas related to public procurements, licenses, taxes, and benefits.

The potential of blockchain to create trusted and transparent public integrity is not just hypothetical. A growing number of simulation studies, pilot projects, and policy assessments suggest its ability to provide audibility directly within public governance infrastructure (Agyeman et al. 2025; Wamba et al. 2024; Verma et al. 2022). Via smart contracts - self-executing code live on a decentralized network - governments are able to automate workflows that require multiple reports, ensure compliance with specific rules at any time in the workflow, and reduce discretion the public servant applying the work flows, or conducting the transactions, can exercise (Li et al. 2024; Nigmatov et al. 2023). Such automation reduces, if not eliminates, the need for intermediaries, increases resistance to bureaucratic red tape, and minimizes opportunities for rent-seeking.

Additionally, the transparency of blockchain allows for real-time visibility. Unlike typical audits, which are sequential and where collateral data can be selectively obscured, blockchain affords a means of continual insights into public transactions and flows of resources (Anywanu et al., 2023;

Bai et al., 2022). Importantly, this transparency is not simply an expectation but rather a significant technical affordance. With both public access and tamper-evidence being afforded by blockchain technology and its distributed architecture, public actors are met with an environment that makes illicit changes observable, if not impossible. This feature serves as an effective deterrent for fraud and misdeeds (Sung et al., 2021; Benítez-Martínez et al., 2022).

Despite these advantages, blockchain use in the public sector is quite limited in scope and scale. Most applications either exist in pilot deployments or proof of concept stages in areas such as voting, land registries, and digital identity (Maolani, 2024; Tyagi et al., 2025; Sharma et al., 2021). The difference between blockchain's potential and its realization can be attributed not just to technical issues but also to legal, organizational, and behavioral frictions that must be considered for the technology to realize its governance-enhancing potential.

The perceived advantages of blockchain in the public sector do not solely result from its technical properties but are also coincident with a larger change in public administration, that is the shift is being recognized as the streamlining of transparency, decentralization, and algorithmic administration. As traditional forms of bureaucracy fail to cope with complexity and increased expectations from citizens, governments around the world are looking for alternative institutional alternatives that emphasize procedural rigor instead of formal discretion (Brinkmann, 2021; Sousa, 2023). Blockchain creates a space where administrative decisions are transformed into protocols that make changes immutable, while also reducing vulnerability to human error and corrupt discretion. This shift marks an important shift in our thinking about governance; a direction away from command-and-control and towards protocol accountability.

In particular, blockchain creates the potential for real-time procedural enforcement using smart contracts. Smart contracts are digital protocols that automatically execute when predetermined conditions are satisfied, without the need for intervention, thus allowing for real-time allocation of public dollars, benefits, services, or similar from an exhaustive eligibility checklist (Li et al., 2024; Kumar, 2024). When implemented in systems using welfare or procurement processes, smart contracts have great potential to reduce the scope for loopholes, minimize discretionary waiting times, and streamline the actions of gatekeepers, who may be able to abuse the informational variance. In this sense, blockchain is more than a transparency mechanism, it is an institutional mechanism for procedural justice to ensure individuals receive the same treatment in the same condition (Jun, 2018; Kshetri, 2022).

This change in governance logic has significant consequences for how we think about public integrity and its manifestations. Instead of focusing only on ex post accountability mechanisms—such as audits or whistleblowers—blockchain can facilitate ex ante integrity wherein malfeasance is structurally impinged before it occurs (Judijanto, 2023; Heckler & Kim, 2020). In essence, blockchain serves as a new actor that, through transparency, verifiability, and rule-enforcement at the data level, reconstitutes the trust-/monitoring balance. Institutions no longer need trust if they can be verified in an ongoing manner with a public ledger.

Additionally, the decentralization of blockchain creates democratic possibilities. Blockchain governance structures can decentralize power among stakeholders, thus lessening institutional power concentration, unlike centralized governance structures that are susceptible to failure or capture (Benítez-Martínez et al., 2022; Pal, 2022). Blockchain can guarantee tamper-proof documentation of input and decisions made during processes in participatory settings such as public budgets or land titling, which can enhance the legitimacy of public actions, but also increase citizen engagement through verifiable inclusivity.

Despite the potential of being a relatively frictionless technology for public governance, technically implementing the approach is not without friction. Administrative cultures, legal frameworks, and organizational routines can often be antagonistic to such radical forms of technological implementation (Batubara et al., 2019; Aliti et al., 2022). Beyond overcoming technical barriers to implementing blockchain, the institution faces challenges posed by institutional inertia, vested interest, and normative doubt, which hamper their ability to create value through blockchain. These types of challenges require strategic governance models that can effectively balance the technical promise of blockchain with contextual legitimacy.

One of the most administratively complex and corruption-prone realms of public governance is procurement. Here, the claim about blockchain's capacity to create a tamper-proof ledger of every transaction, decision point, and contract amendment promises to directly address the opacity created by public procurement that enables collusion, favoritism, and wrongful invoicing, each of which has significantly harmful effects on societal welfare. In a traditional public procurement system, it is not unusual for audit drafts to be selectively edited, or fragmented across multiple agencies. In a traditional public procurement system, to which the public could trace its meaning and legitimacy, every action taken by procurement officials (from publishing the tender to contract execution) would be traced along a publicly accessible blockchain (Balatska et al., 2024; Ibrahimy et al., 2023). Smart contracts may also eliminate false evaluation processes and insincere rules in bidding. Smart contracts can encode bidding rules and compliance checks to create an indisputable event for bids that is accurate and automatically enforced (when programmed).

Another critical area is identity management and citizen registry services. Through Blockchain, decentralized identity (DIDs) systems can be established in which individuals hold ownership over their personal data; however, the government entity can confirm other various attributes with not having to access or store the base data (Sung & Park, 2021; Warkentin & Orgeron, 2020). This practice decreases redundancies in administration, lowers the risks of identity fraud and identity theft. Concerning service delivery, example voting, licensing and distributing benefits, once a verified credential is stored on chain, service delivery can occur quicker and with secured authentication processes regardless of jurisdiction. Public governance also has experiences enhancements in popular financial flows due to blockchain's transparency. Financial transfers for international aid, consolidated fund transfers by government to government, or the public budgeting process have always experienced misappropriation and loss of appropriation. Blockchain’s auditable ledgers for financial disbursement allow every disbursement to be tracked

from the original source to the final recipient; this decreases off the book's manipulation of public funds, and permit funding mechanisms contingent on ethical performance (Friday et al., 2023; Dziundziuk & Dziundziuk, 2022b). It is also possible that the visibility of financial trails within low-trust environments of governance may influence confidence, both domestically and globally.

An additional area significantly altered by blockchain is participatory governance. Cryptographically secured distributed ledgers open new avenues for citizen engagement, such as blockchain-supported referendums, participatory budgeting initiatives, or grievance mechanisms (Bai et al., 2022; Tan et al., 2021). These tools allow for tamper-evident records of wild citizen involvement, and verify that public consultations are inclusive and accountable. Blockchain is especially useful for safeguarding against the post-hoc manipulation of data that often delegitimizes citizen feedback processes. In societies with fragile trust in government, these types of innovations can demonstrate an institutional commitment to fairness, congruency, and inclusivity.

However, the capacity for encoding governance rules into irreversible smart contracts introduces basic and fundamental questions. Who decides how smart contracts function? What legal remedies are available when automatic decision making creates unfair results? Without consistent government or institutional clarity about governance, and systems of legal remedy that reconciles the irreversibility of blockchain with principles of administrative justice, the government risks moving to algorithmic stiffness from discretionary abuse (Brinkmann, 2021; Sharma et al., 2021). These tensions signal the need for mixed-ability governance that incorporates the automation of blockchain with certain legal interpretability and procedural safeguards.

The use of blockchain in public governance is not simply a question of substitution of one technology for another; it is a transformation of the institution. Bordie (2021) points out that for blockchain to provide the benefits and anticipations, we need to rethink fundamental principles of governance: from hierarchies to distributed networks; from bureaucratic opacity to machine-verifiable visibility; from discretionary enforcement to algorithmic execution (Cagigas et al., 2021; Kassen, 2022). The change that blockchain allows and encompasses is consistent with an overall paradigm of governance in the digital era; however, it complicates fundamental institutional, legal, and ethical questions. Movement or behavior is not only about efficiency gains, it is also about changing how authority, accountability, and administrative discretion are distributed in the public realm.

The redistributive aspect of decision-making power is a major challenge in the transformation process being developed. Systems that are decentralized and distributed by blockchain decrease the reliance on centralized institutions to ensure compliance to existing laws, regulations, and policies by removing discretionary compliance through process and increasing enforcement through protocols. This has the effect of potentially increasing consistency and mitigates the ability to 'game' the system. However, the empowering side of decentralized technologies may disempower entities including either the oversight body or citizens in certain edge cases that use

discretion against settled expectations of doses of flexibility, empathic engagement, or interpretation of law (Heckler & Kim, 2020; Benítez-Martínez et al., 2022). The tension becomes more salient in the public sector, where values of procedural justice and responsiveness are explicitly necessary for the degradation of the state's legitimacy through delegated authority. The incorporation of judicial legal procedures into immutable code is something that both adaptive design and law may offer way to address. Further, the implementation of blockchain is less than straightforward in terms of the extreme heterogeneity that is characteristic of public institutions. Governments differ tremendously and present a varied spectrum of considerations when it comes to technical capacity, institutional coordination, expectations about data capacity, and overall maturity of data. The claim of success for one locality or jurisdiction does not suggest ease of transferability to another locality or jurisdiction. Scholars support and encourage a more modular approach that is sensitive to place-based contexts and genuine engagements with public agencies to support incremental adoption of blockchain technologies in a systems style to governance agency, not disuse agency but use in support of the public work, public agency, and ensuring overall value propositions to achieve public policy goals, along with any legal considerations with respect to incorporating blockchain technologies and general citizen expectations (Sousa, 2023; Aliti et al., 2022). For example, municipalities needing to minimize resources or institutional response may benefit more from documents notarized through blockchain technologies or land registry services for property than a procurement system - even when there are still procured resources about land registries and crucial contracts.

One common insight from empirical investigations is that the success of blockchain for governance depends, concurrently, on the existing political economy factors and the technological infrastructure. Vested interests, bureaucratic inertia, and regulatory uncertainty may all interfere with meaningful adoption. Additionally, the benefits of the blockchain can also be captured by powerful actors if access to nodes, governance rights or on-chain data curation are not equitably shared (Brinkmann, 2021; Batubara et al., 2018). This is important because it demonstrates that the blockchain isn't a silver bullet for governance; it is a tool that will have different outcomes depending on the institutional design and alignment of stakeholders.

Ultimately, the promise of blockchain is to create a more verifiable, participatory, and efficient model of governance. However, the promise of better governance will only be realized through meaningful alignment of the technological changes and the institutional changes. Lawmakers cannot think of the blockchain as a plug-and-play solution; they must see it as a new institutional catalyst for governance that creates a tension with normative practice, requires reinterpretation of legal boundaries, and redefines engagement with public accountability (Kshetri, 2022; Judijanto, 2023). Thus, the next iteration of blockchain in governance must include multi-disciplinary research design, significant public consultation, and flexible regulatory experimentation.

In the quest of governments to meet the pending condition of the digital age, the blockchain afford a dissenting view not only in terms of how technology can be operationalized but also in how public authority can be re-legitimated through transparent, citizen-centered, and tamperproof

infrastructure. Nevertheless, implementation is difficult and meaningful uses demand that innovation be governed not only by efficiency or novelty, but establish normative commitments to fairness, inclusion, and institutional resilience (e.g., Gamini et al., 2024). These points are especially relevant in contexts such as public procurement, delivery and distribution of social welfare, and land administration—sectors that have historically suffered from the twin pressures of opacity and discretion, which blockchain infrastructure can provide auditability and procedural re-traceability (Bustamate et al., 2022; Batubara et al., 2019).

Importantly here, we should think and understand blockchain as not a cure for governance but one of several complimentary potential mechanisms that strengthens accountability, rather than replaces, extant accountability mechanisms. The literature has warned of "technological solutionism"—imposing concrete digital architectures onto fluid social processes (Tan et al, 2021, Sharma et al., 2021). In the end, there is likely more benefit in a hybrid model that settles blockchain into the formal enforcement of rules and norms in harmony with the canons of democratic deliberation and public reasoning as an often-privileged space of the public sector.

Implementation of blockchains requires a system of coordination working across multiple disciplines. Literature on blockchain has reflected on the legal approaches/regulatory implications that sit in concert with the immutability of blockchain and one's rights to correcting any wrongs (e.g., Warkentin & Orgeron, 2020; Radonjić et al., 2024). Public administration and public policy scholars note that training stakeholders into the capacity building of digital governance is critical. Technical experts note the need for flexible designs to afford both selective disclosure, computational activity off the chain, and mechanisms to protect and afford privacy (Bai et al., 2022; Ahmed et al., 2024). Some traditional forms of governance have existed for long enough that, notwithstanding technological practices and its ethos, crafting governance systems that can be described as grounded in technology, while at the same time democratically legitimate systems, is possible, but we exist in a convergence of yet independent scholarship that must work together.

In this instance, we note the larger promise of the blockchain for governance may exist in its role as an altogether meta-institution—one that engages public actors in examination of trust, control and authority, and accountability. Its disruptive potential ushers in a space to revise not just the what services are to be delivered, but how authority is to be exercised, who the legitimacy is reaped from, and how to create public value. Thus, the blockchain can perform as more than just a pathway of digital transformation, but serve as a reflective experience on/with the complexity of the competing aspirations of governance.

This dissertation will proceed from this introduction by exploring the institutional viability, legal readiness, and technological readiness of blockchain technology in three jurisdictions: Italy, Canada, and the United States. It will analyze and systematically integrate evidence comparatively to assess the real potential for blockchain to improve corruption risk and make a meaningful contribution to public procurement reform.

1.2 Research Context: Public Procurement as a High-Risk Sector:

Public procurement has become a primary channel through which corruption penetrates public administration, distorts market competition and undermines democratic legitimacy across different political systems and levels of development. Current estimates indicate between 12-20% of GDP is spent on procurement globally (Graycar,2019), and this sector represents not only a large financial tool but also a strategically vulnerable point in the architecture of state governance. The combination of large amounts of money, discretionary power, and multiple actors (including procurement officers, vendors, intermediaries and political appointees) creates a high-risk environment for rent-seeking, favors and institutional capture (Fazekas, Tóth & King, 2016; Hudon & Garzón, 2016).

The risks, threats, and problems within public procurement are not speculative, but have been verified through empirical models and data. Fazekas, Tóth, and King (2016) created a corruption risk index, along with contract-level public procurement data, to compare corruption levels across Europe, and found strong statistical ties between procurement procedures and environments prone to corruption. Their conclusion is that corruption risk related to procurement is not intermittent or anecdotal, but systemic, often built into the rules, thresholds of discretion, and asymmetric information about contract award systems. This is further supported by Ferwerda, Deleanu, and Unger (2016) who assert that procurement corruption must be assessed based on structural indications and behavioral signals, as corruption is both hidden and adaptable.

In addition, procurement transactions are inherently complex, and often involve multi-staged tendering processes or evaluation criteria that can be significantly subjectively perceived and contain technical specifications that are also highly technical (Darabad & Dadgar, 2017; Graycar, 2022), which adds to the challenge of ensuring transparency and accountability. The opacity of these technical and procedural realities provides room for manipulation of the process so actors can conceal favoritism or collusion behind seemingly lawful discretion as a cover. For example, Decarolis and Giorgiantonio (2020) observed recurrent red-flag patterns (e.g. single-bid awards, bidding periods are short, the requirements are crafted) in the same sets of awarded bids when analyzing data regarding public procurement in Italy. Surprisingly, the authors also found that each of these patterns was statistically related to awarding a bid that could have corrupt consequences.

Adding to the vulnerabilities of the structural and procedural weaknesses in the procurement process is the splintering of the enforcement and oversight agencies, usually resulting gaps in enforcement. Hudon and Garzón (2016) describe the use of "entrepreneurial coalitions" by corrupt actors to exploit institutional vulnerabilities by working across bureaucratic walls, political connections and, or suppliers. Entrepreneurial coalitions foster ongoing corruption, and work against procurement systems to shift towards a systemic clientelism where public contracting is a mechanism for patronage not performance. The commonality of "corruption masks" in transitional or developing-economies does not preclude vested interests in mature rule-of-law administrative states displaying corruption in procurement—legally or illegally (Fazekas & Kocsis, 2017).

What makes public procurement distinct from administrative processes more generally is not only the scale of resources mobilized, but also the latitude for decision-making allowed to public officials. Fazekas and Kocsis (2017) highlight, in their comparative study, how the risk of corruption is greater in environments where formal procedural safeguards exist alongside informal, often opaque, influence processes. In this situation, high-level corruption does not necessarily run afoul of written rules but rather engages procedural flexibility – such as using non-competitive bidding, having specifications that are bespoke, evaluation criteria that are not public, and so on – to achieve private or political ends. This kind of action compromises the impartiality, competition, and efficiency that procurement processes are designed to be based upon.

The multi-stakeholder environment of procurement character - in its layers of ministries, contracting authorities, auditors, suppliers, consultants, and political actors - routinely allows for collusion and networked corruption for procedural flexibility. As mapped by Fazekas, Sberna and Vannucci (2021) public procurement is typically controlled not only by formal regulations but also through extra-legal arrangements where actors exercise rule-bending behavior based on shared understandings without any explicit violation of law. The nature of these arrangements is often untouchable by oversight as they become established aspects of institutional practice and political patronage. The engagement of public procurement organizations creates structural pathways for both routine corruption and strategic corruption where external scrutiny is locally absent or fragmented.

Empirical insight from both high- and low-capacity governance realities suggests that the risk configuration of procurement corruption is not subject to specific jurisdictions, but rather is reoccurring structurally. Falcón-Cortés, Aldana and Larralde (2022), studying procurement systems in Mexico found that a new political leadership need not be characterized by a cleaner contracting system if the underlying procurement processes are still being manipulated, even if through procurement systems that are not susceptible to manipulation. Similarly, in a resource poor environment such as Uganda, procurement has become a contestation point for systematic corruption, with required institutional reforms due to corruption, going beyond rule adherence to case purpose branding (Basheka, 2021). Such findings re-enforce the position that procurement represents not only an administrative challenge, but a space of contestation between integrity and abuse of power that deserves scholarly and policy attention.

Indeed, the impacts of procurement related corruption go beyond flawed budgets. In their analysis of pharmaceuticals procurement, Kohler and Dimancesco (2020) explored the cause and effect of corrupt practice with direct implications for public health outcomes through tendering and supplier selection, access to medicines and equity of service delivery. In the infrastructure and construction sector, Bhagat and Jha (2023) whet departed on misallocation of contracts due to corruption, impacts on project quality and completeness, and quality of service, ultimately highlighting the longer-term sustainability of projects which many communities remain unable to benefit from. The sectoral illustrations confirm that procurement corruption does not only waste public funds but also repurposes developmental futures and renders almost ineffectual the goals of public spending.

The urgency of addressing corruption in public procurement arises, not only because it is both a pathway to value creation for the public and a means to exploit by the elite, but because procurement risk is systemic. Procurement risk is systemic in character and provable within cross-national corruption indicators and with unique across contract analysis. Therefore, we require tools that are NOT simply punitive or reactive, but diagnostics and preventative. Gallego, Rivero & Martinez (2020), state that by being able to identify corruption before signing the contract, through early warning systems, procedural flags and anomalies, will shift public procurement oversight and action from a reactive approach to a proactive governance system. These depend on granular, contract-level data and operate in the belief that corruption contravenes predictable behavioral and procedural expectations. This behavior is the basis for many observable patterns that can be mapped in multiple empirical settings. Decarolis & Giorgiantonio (2020), in their analysis of thousands of tenders in Italy, mapped procurement corruption to behaviors including poor competitiveness (such as winning tenders by single-bid), limited bidding period with submission clearance, and repetitive awards to connected firms. These behaviors often distil into technical parameters that once aggregated most of these behaviors can be predictive proxies for underlying procurement corruption, even if there are no breaches of formal process. Similarly, Lyra et al. (2022) have shown that data-driven detection systems, and in particular with machine learning and network analysis, can track collusive behavior and favoritism. Implicit in these findings is the suggest that corruption in procurement is computable, if monitoring systems are able to ask questions of compliance as well as operating regularities. Yet, detection on its own cannot take the place of systemic safeguards. Graycar (2022) stresses the importance of reframing conventional principal-agent models that have defined the public sector's conceptualization, especially in procurement, as actors, when operating in that space, have a potential to wear multiple and overlapping hats simultaneously—gatekeepers, beneficiaries or enablers of corrupt behaviors. The basic assumption of stable and common institutional roles is also complicated by the ways in which responsibilities may be distributed across various sub-agencies, which can themselves lead to jurisdictional gaps, enforcement gaps, and related problem. The challenges are compounded by Chabrost's (2020) observation that institutions divert any attempts to respond to corruption by limiting legal expectations to dated and in some cases outdated legislation and taking procurement to be insulated administrative process. To summarize, public contracting can be seen as often related to corrupt behavior not due to rule breaking, but just as often as not personally compromising regulations, and best practice and policies, in ways that garner legal protection but undermine normative effect.

Understanding the implications, reform has tended to progress with policy and academic consensus suggesting that increasing structural transparency, along with procedural standardization, and increasing institutional coordination, is often the best approach to decrease corruption in general. Nonetheless, within these reforms, we may run into limits. For example, Adjorlolo et al (2025) provided AHP-based assessments of procurement stages that are structurally inefficient and thus systemically conducive to corruption (e.g., needs assessment, bid evaluation and contract monitoring) that represented more corrupt environments regardless of institutional context. This

should signal the need for intervention at certain stages that bring together legal, organizational, and technological levers in a joint fashion. While excessive regulations generate inefficiencies, lack of enforcement ultimately fosters impunity.

Procurement-based corruption has been the subject of considerable legal reforms and transparency initiatives, yet it continues despite normative arguments for formal accountability. This suggests that formal rules and institutional structures, in and of themselves, do not adequately mitigate this behavior.As Fazekas and Wachs (2020) have shown, corruption will change form to meet institutional constraints. Corruption can be seen in new forms like network favoritism, revolving door appointments, or clustering of contracts - whereby firms with connections to political elites obtain a large unauthorized share of public tenders through opaque processes. Even in jurisdictions with strong administrative controls, like parts of the European Union, corruption can remain deeply hidden in not-truly competitive markets which possess incoherent regulatory regimes, or where oversight is fragmented, and the data used to inform public accountability processes is weak.

Additionally, there may be structural mitigated risks associated with inter-jurisdictional variation with respect to operational mechanisms. Like Italy, countries with structural challenges including complex regulatory systems, discretionary agency decisions, and lack of monitoring contract administration, are particularly vulnerable to systemic corruption and episodic corruption (Lisciandra, Milani, & Millemaci, 2021). Work conducted by Decarolis and Giorgiantonio (2020) document variations of risk indicators including non-competitive award and repeated contracts with the same contractors across almost all municipal bids was apparent at the time with little subsequent efforts to mitigate these risks with formal or informal acceptance of EU procurement directives. While we might view Canada and the United States' corruption risk to be low as indicated by historic comparatively better rule-of-law indicators, they too face structural systemic corruption risk. Analyzing Swedish-style procurement markets, Wittberg and Fazekas (2023) demonstrate structural vulnerability relates specifically to imperfect competition and contractor consolidation opens up multiple avenues for collusion surrounding bid-level processes that align with procurement context but may subvert intended higher-order goals by public contracting that aims at fostering competition within the procurement context.

That different corruption indicators exist across different jurisdictions from bid-rigging in southern Europe to systemic corruption in construction projects in Canada and the US indicates that they may not be incidental, rather, the confusion in largely fragmented public accountability systems is likely explained by institutional structures - Bhagat and Jha (2023) went so far as to suggest this structural risk is universal, limited to context-variant decisions made by bureaucrats and/or contracting agents in response to system strain (Sharma, Sengupta, and Panja, 2019). For example, Sharma et al. mapped specific vulnerabilities throughout the procurement process noting stages such as shortlisting bidders and performance monitoring as consistently hazy and under-regulated. These patterns of vulnerability justify an academic and policy shift from episodic to systemic design flaws.

In reaction to these systemic concerns, speculation has turned to identifying many possible 'innovative governance' approaches that address steady structural production risks, rather than simply relying on retrospective audits or discretionary audit investigations for public procurement. Many jurisdictions are currently establishing processes with procurements built-in real-time monitoring, automated verification and immutable record keeping (Velasco et al., 2020). These renewed demands for structural reform have raised the idea of utilizing digital technology - most notably, blockchain-based technologies - as a way to help improve procurement transparency, accountability, and auditability. Though digital technologies may not be a "magic bullet," they allow us to conceptualize procurement governance as a technologically mediated process based on verification that is hardened to "discretion."

With these global challenges converging, the research and policy case for prioritizing procurement within anticorruption strategies has become both empirically grounded and normatively timely. As Kohler and Dimancesco (2020) highlight in the realm of health sector procurement, the costs of corruption relate to more than just inefficient use of public money - they relate to loss of lives, reduced public services, and increasing social inequality. These harms become magnified when we consider public procurement activity in broad high-value, high urgency contexts such as infrastructure, military, pharmaceuticals, and disaster recovery that require attending to the tasks of speed, complexity, and accountability. During emergencies like the COVID-19 pandemic, Gnaldi and del Sarto (2024) indicated that the risks associated with corruption in procurement increased substantially—supervisory processes became weaker and reduced legal exceptions were exploited. This highlights the contingent nature of corruption risk: variables of political and economic context along with institutional design have consequences for corruption risk.

The resilience and variability of corruption in procurement, in context, showcases the limits of established reforms based largely on institutional rules, training or punitive enforcement. Similarly, even established transparency portals or e-procurement are all weak due to lack of integrity of the associated data, and weak enforcement mechanisms that are consequently unable to help administer compliance on real-time evidence. As such, governance approaches that paired distributed ledger technologies DLTs such as blockchain offer an avenue for reconceptualizing oversight and ethics in the public procurement process. Velasco et al. (2020) describe aspects of blockchain for having traceability embedded; smart contracts that indicated enforced immutability and automation of compliance—the public procurement cycle could potentially also be deemed auditable and de-facto immutable in nature.

However, the implications and the effective transformations in refining governance via DLTs and blockchain are not equal across all jurisdictions. Differences in legal compatibility, regulatory architecture, and digital infrastructure affect how countries can effectively manage legal systemic risks. While Italy's complex legal traditions and fragmented oversight structures encounter challenges, such as Canada's federalized systems of procurement and many agencies in the United States,' must use a different lens. The comparative frameworks require an understanding of legitimate differences in contexts, while contextualizing aspects of illegitimacy or illegitimacies that expose vulnerabilities and also possibilities for reform. To borrow an argument from (Basheka, 2021), if reforming sustainably against corruption in public procurement, institutional coherence and innovative technologies matter.

This dissertation is based on the filters mentioned above. It understands public procurement as having structural risks that can be exacerbated by institutional fragmentation, opacity of law, and discretionary governance. The dissertation optimistically argues that blockchain technologies, with sound legal-regulatory designs can improve integrity in a vital public process. The goal of the dissertation is to compare three democracies, Italy, Canada, and the United States and consider legal, regulatory and future technological capacities needed in the public sector to reduce risk of corruption procurement contracting. The following sections continue with the argument, starting with a critique of the research-based corruption in public procurement and local experiences using blockchain in a range of governance tools.

1.3 Research Gaps:

While the literature continues to expand concerning the theoretical advantages of blockchain in terms of facilitating transparency and accountability, there is a significant research gap in comparative and contextual studies that examine how blockchain technologies are influenced by national legal, regulatory, and institutional environment. Much of the literature evaluates the technology in a single-jurisdiction case, or even conceptually, but does not answer how adopting the technology would function with these differing public procurement regimes across legal traditions, such as civil and common law, characterized in this research. The lack of a comparative research agenda limits our understanding of how blockchain operates across various governance architectures.

In addition, the literature rarely distinguishes between a legal framework and regulatory approaches - these are often considered together as a single layer of analysis, and the dynamic functions of policy experimentation, regulatory sandboxes, and administrative discretion to encourage or inhibit public procurement of blockchain is a point of under-researched - particularly for countries with legal permissibility, but bureaucratic community inertia and lack of regulatory innovation limited practical implementation.

A lack of granularity also exists around understanding corruption vulnerabilities in procurement systems. Existing studies are primarily framed around the broad conception of how blockchain can resist corruption, very few studies use fewer concrete descriptions to study the how specific blockchain functions (e.g., smart contracts, audit trail, decentralized registries) align with specific corruption typologies e.g., bid rigging, opaque payments or collusion. Without this mechanistic clarity, proposed solutions will remain speculative.

Ultimately, contemporary research insufficiently considers institutional and sociopolitical resistance to the implementation of the blockchain. Issues of digital capacity, bureaucratic risk aversion, and power asymmetries are often disregarded completely, yet these are some of the most important factors relevant to the diffusion of any public-sector technology. There have been few studies considering adaptive policy transfer—the extent to which jurisdictions can learn from each other while adapting blockchain governance models to their local legal, technical, and political contexts. The majority of policy recommendations assume that there are linear, one-size-fits-all solutions and do not consider the messy realities of how and why innovation diffuses from one country to another.

1.4 Research Novelty:

This dissertation attempts to fill these gaps by providing an interdisciplinary, comparative, and mechanism-based analysis of blockchain's anti-corruption potential in public procurement across three legal jurisdictions: Italy, Canada, and the United States. The first contribution of this dissertation is the proposed forms of a three-dimensional analytical framework that separately and distinctly evaluates legal, regulatory, and technological qualities contributing to national context in each jurisdiction. Whereas previous research combined law with regulation, or did not considerate administrative governance at all, this study distinctly separates, and evaluates in a systematic fashion, the formal legal and statutory basis, contextual and dynamic policy instruments, and technological development of blockchain scripting conditions.

Second, the study provides a typology of corruption specific to procurement that is directly matched with applications of blockchain technology. Instead of making vague statements about the use of blockchain for transparency, the study considers how specific functions of blockchain as smart contracts, timestamp Bidding logs, or role-based permissions address identifiable risks in the procurement workflow. This level of specificity provides detail on a much finer-grained level of mechanism-risk fit, increasing the utility of the research.

Third, the research includes a strong actor-level and institutional level of analysis highlighting how implementation is influenced by digital readiness, bureaucratic norms, and resistance from vested interests. By foregrounding these socio-political conditions, the dissertation situates blockchain governance as not just a technical solution - but as a negotiation at an institutional level involving political economy and administrative culture.

In conclusion, the dissertation offers a n model of adaptive cross-jurisdictional learning, finding that blockchain adoption cannot take place through replication alone. It identifies a framework for contextual policy transfer which would allow legal and regulatory insights from a country, to guide but not bind, the course of that journey in another country. The dissertation also fills the gap in blockchain governance research, which is significantly lacking adaptive, scalable and realistic models of international learning.

Together, these contributions place this study as an original contribution and as significant to the body of literature on public law, digital governance and anti-corruption reform in the empirical real world of practice, while taking both the systemic complexity and institutional variety into consideration and management.

1.5 Research Objectives:

1.To map and compare the prevailing legal frameworks in Italy, Canada, and the United States that relate to blockchain adoption and anti-corruption in public procurement.

2.To map and compare the current regulatory frameworks and policy initiatives related to blockchain adoption and anti-corruption in public procurement in Italy, Canada, and the United States.

3.To identify specific corruption vulnerabilities in the public procurement process and examine how blockchain technology has the potential to improve transparency and accountability in addressing those vulnerabilities in selected case studies from Italy, Canada and the United States.

4.To examine the technical feasibility of blockchain solutions and existing technological approaches and its challenges for implementation in relation to anti-corruption frameworks in public procurement in Italy, Canada, and the United States considering socio-political contexts.

5.To assess opportunities and challenges for cross-jurisdictional learning and adaptive transfer of adopting blockchain-based anti-corruption strategies in public procurement in Italy, Canada, and the United States.

1.6 Research Questions:

1.What are the major legal statutory and jurisprudential provisions related to the current constraints and potential opportunities for using blockchain technology for anti-corruption as applied to public procurement in Italy, Canada, and the United States?

2.What is the differing/resembling regulatory frameworks and policy initiatives related to the adoption of blockchain and anti-corruption efforts in public procurement in Italy, Canada, and the United States?

3.What are the particular corruption vulnerabilities in the public procurement processes of Italy, Canada, and the United States, and what role may blockchain technology play as part of concrete mechanisms to provide transparency and accountability to operate effectively in such instances- e.g., in the hard commodity procurement context?

4.What are the key technical challenges, opportunities, and particular technological features associated with developing blockchain solutions as part of an anti-corruption effort within public procurement environments of Italy, Canada, and the United States, including socio-political conditions, actor resistance, and the trade-offs associated with various blockchain typologies?

5.What are the core points of comparison, learning and barriers experienced in Italy, Canada, and the United States with respect to adaptable models and pathways related to cross-jurisdictional learning barriers in the context of widespread adoption of blockchain-based anti-corruption mechanisms in public procurement?

1.7 Research Hypotheses:

1.The legal frameworks in Italy, Canada, and the United States, despite their foundational differences (civil vs. common law, federal structures), present identifiable commonalities and divergences that significantly influence the potential for blockchain adoption and its effectiveness for anti-corruption in public procurement.

2.The regulatory approaches and policy initiatives in Italy, Canada, and the United States exhibit distinct patterns regarding their support for, or resistance to, blockchain integration in public procurement, influenced by varying governmental attitudes and institutional capacities.

3.Blockchain technology, when appropriately designed and implemented to target specific public procurement vulnerabilities, can demonstrably create opportunities for reducing corruption by enhancing transparency and accountability, particularly through immutable audit trails, transparent bidding, and automated smart contracts, in selected case studies across all three jurisdictions.

4.The technical feasibility and specific technological approaches to blockchain implementation in public procurement vary across Italy, Canada, and the United States due to differing infrastructure maturity and institutional readiness, with their success significantly mediated by socio-political factors, actor-level dynamics, and the inherent trade-offs of different blockchain typologies.

5.Adaptive learning from blockchain initiatives in public procurement is feasible across Italy, Canada, and the United States, but successful transfer requires careful contextual reinterpretation, accounting for differences in legal, regulatory, technological, and socio-political landscapes rather than mere replication of models.

1.8 Scope and Limitations of the Study

This study adopts an intentional overextension mitigation strategy. To be methodologically rigorous and analytically deep, this study limits the empirical scope to public procurement—defined in the literature and described in international policy as one of the "most vulnerable sectors to corruption" in the world. Therefore, instead-of providing a low level, broad-spectrum, superficial analysis of whole national procurement systems, the research take a targeted sub-sectoral approach of the public procurement system across each jurisdiction. The research focus on specific procedural stages in the procurement process that are characterized as high-risk, including tender development, evaluation, contract execution, and payment verification which are precisely the points in procurement where discretion, ambiguity, and wiggle room have always existed to facilitate corrupt activities. Where permitted by data availability and access, the research may be narrowed further, to one or two case studies, for example, the procurement practices of a specific federal department or the contracting regime of a particular major municipality. Therefore, by justifying a narrowed level of analysis, the purpose is a richer, more contextualized understanding of the key institutional, legal, and technological forces at play, while sidestepping the analytical dilution of over-extended comparative approaches.

In accordance with the concept of the study, the technological lens is prioritized to blockchain systems as anti-corruption vehicles, intentionally excluding any other tech or non-tech anti-corruption interventions, like whistleblower platforms, traditional e-procurement systems, or institutional reforms effort to achieve conceptual and analytical coherence. The focus of the research will solely be directed towards blockchain's main features—immutability, decentralization, traceability, and automation via smart contracts—as attributes that can, relative to their gaps, address vulnerabilities in procurement.

Because quantifying corruption outcomes is particularly challenging, the study recognizes the two-fold challenge of quantifying the causal change in fixed metric corruption experienced via blockchain adopting technological procedures, especially given that a substantial portion is qualitative inquiry. The section focus on identifying, conceptualizing, and explaining how blockchain may produce greater transparency, improved accountability, and reduced space for illicit activity. These mechanisms would be identified, conceptually discussed, and analyzed as their warranted, using triangulated publicly available procurement and policy documents, primary documents, legal and policy documents, and semi-structured interviews with three practitioner, regulator, and relevant subject matter experts to justify both methodological feasibility as well as analytical excellence, while acknowledging the limitations of relying on publicly available sources and potential inability to access sensitive, classified, or proprietary data.

2. Literature Review

Methods and Sources (Literature Review)

This chapter presents a narrative, structured review of blockchain and other distributed-ledger technologies (DLT) usages for enhancing integrity and transparency in public procurement by establishing an audit trail. The review is designed comparably across Italy (as a member of the binding EU acquis), Canada, and the United States during a time frame of 1 January 2010 to 13 August 2025. This time frame encompasses permitted and hybrid architectures; evolving legal frameworks for procurement datasets and the digital records; and a plethora of pilots relevant to e-procurement systems. To make evidential weight transparent, any source will be tagged where first mentioned as empirical [E] or, prototype/technical or conceptual [P/C], or legal/doctrinal/ primary law [L/D].

Peer-reviewed literature was collected mostly from Scopus and the Web of Science Core Collection, with a somehow uses of Google Scholar to check coverage and find hard-to-index items. For legal and doctrinal materials, EU primary and secondary law were sourced from EUR-Lex, while legislation, regulations, and case law were from Westlaw/Lexis. Institutional portals (e.g., ANAC, European Commission, OECD, and World Bank) were used for bounded grey literature describing procurement policy and process, institutional arrangements, and guidance on regulation. Sources are primarily English, while Italian-language sources and EU legal texts were included when needed to contextualize Italy's normative environment.

The search strategy merged three sets of constructs: public procurement; integrity and corruption mechanisms; and DLT affordances. A typical Boolean string, modified by database and employed on titles/abstracts/keywords, was: (“public procurement” OR tender* OR “government contracting”) AND (corruption OR collusion OR “single-bid” OR “bid rigging” OR integrity OR transparency OR audit*) AND (blockchain OR “distributed ledger” OR DLT OR “smart contract*” OR “hash anchor*” OR “zero-knowledge”) AND (Italy OR Italia* OR EU OR “European Union” OR Canada OR “United States” OR U.S.). The secondary passes added lifecycle and legal refinements, including “e-tendering,” “bid submission timestamp,” “change order,”GDPR, MiCA, FAR, and “Treasury Board,” for jurisdictional specificity and lifecycle stage-specific contributions recovery.

Eligibility criteria were established ex ante. Included were (i) peer-reviewed publications about public procurement and DLT using any methodological approach; (ii) original legal and doctrinal materials on procurement documents, digital signatures, smart contract enforceability, and data protection; and (iii) credible institutional documents used only to define procurement contexts or legal frameworks. Excluded were generic crypto/fintech or supply-chain studies with no

identifiable relation to procurement, unverifiable website material, duplicates, and purely conceptual e-government materials unless they offered clarification of a procurement-stage mechanism. Screening was conducted in two phases, title/abstract and full-text. For each included document, a structured extraction framework recorded the bibliographic detail; jurisdiction; actor category (contracting authorities, oversight organizations, bidders/consortia, intermediaries); procurement lifecycle zone (planning, posting, bidding (submission), evaluation/award, execution, payment/audit); corruption mechanism (e.g., bid rotation, alteration of timelines, change-order manipulation); DLT function and type (immutability, verifiable posting, timestamping, conditional payment/escrow; public/permissioned/hybrid; legal pinch-points (e.g., right to erasure and access by data-subject, admissibility of blockchain evidence, enforceability of smart contracts); source tag [E/P-C/L-D]; and main findings and limitations. This framework facilitates like-for-like comparison across jurisdictions and prepares the reader for the mechanism comparison that will follow.

The process of synthesis has two analytic dimensions. The first is the procurement lifecycle, tracing the match of the particular functions of DLT with stage-specific integrity risks across planning, publishing, solicitation, evaluation/award, execution, and payment/audit. The second analytic dimension is the actor perspective, which illustrates how contracting authorities, oversight bodies, bidders/consortia, and intermediaries create, alter, or verify records, as well as how DLT changes their rights and obligations to information. Our findings are reported as discrepancies rather than reconciled. Ongoing tensions in law and technology—especially those between the immutability of the ledger and data-subject rights—are captured as design constraints and connected to implementable governance and architecture choices, including reliance on off-chain storage with proofs on-chain, selective disclosure, and zero-knowledge attestations.

Grey literature is utilized sparingly and only seen as a supplement—not a substitute for—peer-reviewed or primary legal sources of information. The review employs backward and forward citation tracing from the anchor studies to minimize selection and confirmation bias; the review is jurisdictionally balanced across Italy/EU, Canada, and the United States; the review logs decisions to include and exclude information explicitly. These measures improve transparency and replicability; thus, ensuring the review's synthesis will be academically sound, and offers a direct response to the thesis's inquiry about the comparative possibilities of how blockchain can augment integrity in public procurement mechanisms.

2.1 Conceptualizing Corruption in Public Procurement

Corruption in public procurement is neither a marginal phenomenon nor a sporadic failure of governance; it is seen as a systemic corruption and ongoing pathology of the modern and social regulatory state accountability. Corruption by its definition is understood as the "misuse of public trust and entrusted power for private benefit" (Rose-Ackerman & Palifka, 2016; UNODC, 2013). This unethical wrongdoing diminishes public trust, undermines market operations and waste

precious amounts of public resources. It has been estimated that between 10% and 25% of public expenditure is lost as a result of corrupt practices each year, globally (UNODC, 2013). Public procurement is a crucial government activity which typically represents around one-third of all government expenditure, representing a significant portion of overall national GDPs, and is particularly susceptible to corruption for the following reasons; there are large amounts of money flowing, processes are often necessarily complicated, and public officials are often afforded significant discretionary power (Siino, Iezzi & Gara, 2024; OECD, 2016). Anderson, Jones, and Pereira Neto (2024) offer an extensive explanation as to why forms of procurement are particularly easy to corrupt and for collusion to occur, highlighting the harm payoffs can cause and the extent of the problem of all forms of corruption and collusion persists despite international and national attempts to intervene. The problem is particularly acute in places such as Italy, where corruption has been linked to organised crime and where large amounts of European Union funds are being allocated for infrastructure and reform (Siino, Iezzi & Gara, 2024).

In Canada, fragmentation between federal and provincial/municipal procurement regimes yields heterogeneous oversight intensity and data granularity, which has implications for comparability and enforcement pathways. In the United States, federal rules (e.g., the FAR) coexist with varying procurement codes in states that produce disparate procedural design, bid transparency, and remedies.

The literature review is narrative in nature, and considers blockchain/DLT only as it pertains to integrity, transparency, and auditability in relation to public procurement. Sources are identified through targeted searches of multidisciplinary databases (e.g. Scopus, Web of Science) and legal repositories (e.g. EUR-Lex, Westlaw), as well as through backward/forward citation tracing. We privilege procurement-specific empirical studies and primary legal resources; only in instances where the elements pertain to procurement and are not non-procurement-focused e-governance, and/or fully conceptual, do we cite those sources. Upon first mention, we label each source as empirical, prototype/conceptual, legal/doctrinal to denote the weight of evidence.

In traditional legal and economic theory, corruption is commonly understood within the framework of the principal–agent or agency problem, where public officials act as the agents of the state and pursue private benefits instead of acting in the public interest their principals—taxpayers and the citizenry—entrusted to them. Through early commitment to the currency of this construct in legal theory, this framing has been popularized through the writings of researchers such as Rose-Ackerman (1975, 1999), and subsequently refined in regulation and governance literature, conceiving corruption as an opportunistic deviation motivated by asymmetric information, poor accountability tools and systems, or simply because of weak sanctions (Jones & Pereira Neto, 2020). Despite being a powerful and explanatory model in political accountability and regulation, the principal-agent framework lacks theoretical rigor to explain understanding when corruption is pervasive, acceptable, normal, or regularized in political institutions. Enduring engrained patterns of corruption—even under more digital contexts—exhibits that the technological fix does not always fix the socio-political and institutional dimensions to malign this conduct (Transparency

International, 2024). Perhaps most crucially, an anti-corruption perspective admits to the type of opposition reinforcing corrupt practices as simply being instrumental or habitual, and an extension of the prior observations surrounding institutional isomorphism, principled or structural legitimacy may appear in reform that does not address a more politically predicated set ethos. This leads to change that is not hypothetical—institutional isomorphism theory suggests organizations engage or append into structures or processes, not necessarily for instrumental efficacy, but instead in the sense of orthodoxy, or simply as something to do, becoming a symbol of adherence without a substantive intervention or change in ethical values as to be normative, especially after the reforms leave the academic discussion too, leading to superficial or habitual schemas of organizational change (DiMaggio & Powell, 1983).

More recent literature has introduced the collective action problem as a significant alternative perspective. Collective action theorists contend that when actors in the system believe that corruption is the normal state, the perceived costs and risks of remaining uncorrupted (or speaking out) is weakly constrained or structurally diminished (Rothstein, 2011). In these types of environments, reform efforts, even if as sophisticated as something like monitoring and punishment, do not change the belief systems that incentivize corruption. There is an emerging view that when citizens in Brazil view corrupt acts as a necessary condition, it negates even rational deterrence frameworks (Jones & Pereira Neto, 2020). Where corruption is systemic, it creates a self-sustaining equilibrium in which both public actors and private actors collaborate, not merely to enhance both of their pay offs, but also have a rational expectation that resisting would either be futile or represent a net cost. The notion of "proximity" between firms for example, reduces the transaction costs associated with entering into inter-firm corruption to support collusive behaviors that undermine fair or competitive behaviors in contexts of uncertain markets (Troisi & Alfano, 2023). Hajnal (2025) even notes that in competitive authoritarian regimes, rationally utility-maximizing actors, can choose an intentional effort to either limit or promote types of corruption, based on a rational risk/cost-benefit analysis regarding the benefits to the regime; the regime may like some acts of corruption while seeing the efficiency in preventing other acts of corruption due it costs or risk to their regime.

This conceptual overhaul, from rational-choice opportunism to norm-driven equilibrium, contributes to our understanding of procurement governance in important ways. Under the collective action model, corrupt practices cannot solely be explained by weak laws or lack of enforcement; corruption must be rationalized as a governance outcome in which state institutions are captured, procurement laws subverted, and procurement oversight made performative. Empirical problems with procurement governance including Brazil's Operation Carwash (OCW) epitomize this argument. The multi-billion-dollar scandal involved a hyper-complex procurement cartel involving state-owned enterprises (SOEs), construction conglomerates, and political elites, where procurement laws were not absent – procurement regulations were purposefully used as a facade to provide a veneer of legality while colluding behind the scenes (Jones & Pereira Neto, 2020). This provides important insight into the institutional entrenchment of collusion in high-

level procurement systems in which corruption and collusion can become mutually reinforcing and therefore stable and entrenched.

The definitional parameters of corruption in procurement needs clarification. Fazekas, Tóth and King (2016) offer a definition in which they define corruption in procurement as the intentional bending of procurement rules and principles to favor closed networks, systematic exclusion of competitors and awarding of contracts with bias. This perception is essential for identifying the line between low competition due to market failure, and low competition due to intentional action. The latter situation described is not simply regulatory failure when the behaviour is repeated and enabled institutionally, it is a corrupted procurement regime. The presence of one offer in a tender for example, is in automatic high indication of a lack of bidding competition (Siino, Iezzi & Gara, 2024; Fazekas, Tóth & King, 2016). Legal research can increasingly support this view arguing that procedural legitimacy e.g., public tendering, technical scoring etc., can be manufactured as shams to disguise the rigged nature of the outcome.

The present study implements procurement-specific “red flags,” entailing six observable risk indicators that warrant greater attention for integrity risks. First, single-bid tenders can be interpreted as an indicator of stifled competition. Second, short and/or inconsistent publishing timeframes can limit competition and contribute to a lack of bidders. Third, consistent co-bidding by the same group of firms can indicate potential cartel co-action. Fourth, procurement awards of prices that are significantly different than the engineer estimate or based on comparable contracts can indicate potential overpricing. Fifth, uncertainty in processes will be indicated by a degree of discretionary exceptions beyond institutional baselines. Sixth, a significant increase in the frequency and/or value of change orders during execution can indicate ex-post rent extraction.

In the subsequent analysis, we connect each indicator to a relevant blockchain or DLT control, as well as an examination of the jurisdictional conditions necessary for permissible use in Italy/EU, Canada, and the United States. Roles and controls for time stamping, such as verifiable timestamping helps to interrogate notice periods; commit-reveal mechanisms can needed to preserve confidentiality and to address subsequent changed bids; the on-chain hash is additive to document integrity without exposing PII; and append-only audit trails enable full traceability and post-award analysis. The legal review by jurisdiction analyzed the evidentiary rules around digital records, electronic signatures and record retention, data-protection limitations, and the authority of contracting authorities to use the respective controls.

Despite this conceptual commonality, jurisdictional differences matter. In civil-law Italy, conduct procurement is largely codified through Directive 2014/24/EU and the Codice dei contratti pubblici (d.lgs. 36/2023). Federal procurement in the U.S. has no such procurement codification, using the FAR as the source for ex ante procurement rules (contracting officers, for example, are responsible for ensuring 'fair and reasonable' pricing), while enforcement occurs ex post through the False Claims Act (FCA or 31 U.S.C. 3729-3733). The Canadian federal procurement regime

has more procurement rules but operates within a framework of federally published procurement rules defined by the Directive on the Management of Procurement (2021-) supplemented by tools at the provincial level. What is common across all three regimes is their evidentiary consideration of the status of electronic records and signatures in law: eIDAS (EU/Italy), ESIGN/UETA (U.S.), and the Canada Evidence Act, which is crucial for blockchain-related auditability. Recent research out of Italy has reviewed potential open-data-based indicators for risk associated with procurement, and while it identifies areas of persistent risk and risk vulnerabilities, it also refrains from making sweeping statements about political interference. Anderson, Jones & Kovacic (2024) emphasized comparative-implementation challenges and context-sensitive thinking when designing and implementing procurement.

Efforts to combat corruption must therefore grapple with not only legal reform but also institutional design and cultural change. Transparency International (2024) underscores that even when procurement laws are formally aligned with international standards such as the UNCITRAL Model Law or the United Nations Convention Against Corruption (UNCAC), particularly Chapter II, Article 9, their enforcement often falters due to political patronage, administrative opacity, and limited civic oversight. The implication is that corruption resilience is not a function of legal instruments *per se*, but of the interplay between institutional autonomy, political will, and the activation of monitoring actors—including civil society, media, and auditing bodies. The limitations of focusing solely on structured procurement data have been noted, as textual information in tender documents is often used by corrupt actors to hide favoritism through subtle, technically complex conditions, suggesting that text mining has the capacity to advance understanding of corrupt behaviors (Katona & Fazekas, 2024).

As anti-corruption frameworks progress, scholars have suggested hybrid approaches (combining legal, political and technology pathways), such as relying on digital procurement platforms, open contracting data standards, and blockchain audit trails to maybe reduce discretion and notability (Transparency International, 2024; Mutungi, 2023). But as Soleiman (2017) points out, these tools will only succeed if there is institutional capacity to act on anomalies and alerts. In the absence of credible enforcement (with real judicial independence), nothing but transparency will disrupt the structural reproduction of corruption. So here again the literature comes to a convergence of thought: legal reform is necessary but not sufficient in addressing corrupt practices. Systemic changes to tackle corrupt practices should consider corruption as political economy and not simply as legal anomaly. Anderson, Jones, and Pereira Neto (2024) support this argument in their work, arguing that public procurement systems need to be continually honed and developed to counter positive incentives, block opportunities, and create compliance. Therefore, in this thesis, blockchain is examined as a control and assurance layer that adds to, not replaces, procurement statutory controls, oversight institutions, and enforcement capacity.

The process of understanding corruption in public procurement involves reconceptualizing corruption as a complex system rather than as a binary model of compliance versus deviance. To do so, we need to implement a pluralistic framework that reconsiders structural incentives,

diffusion of norms, institutional fragility and legal plurality. The study of corruption in procurement is contested space which wrestles with various unresolved tensions, such as the degree to which legal forms, norms of behaviors, and political dispositions each determine the potential for corruption in procurement systems. Until those gaps in theory and praxis are addressed, the current study will assess how blockchain-based procurement solutions might disrupt corrupt equilibria in three very divergent cultural and legal regimes, Italy, Canada, and the United States, which each show distinct institutional and normative configuration. The literature on corruption in public procurement has produced a range of typologies and explanatory models, but upon closer inspection there appears to be significant variance in the degree of rigor and appropriate contextualization across studies. In particular, while early foundational studies that have used governance indicators from the World Bank, or the Corruption Perceptions Index (CPI) from Transparency International, provide broad comparisons, they also conflate perception-based surveys with actual misconduct levels. This conflation poses significant challenges for proper and appropriate analysis because they do not give a lot of nuances to procurement systems within cultures, where corruption is largely hidden, and unreported. This problem has been identified in meta-analyses (e.g., Fazekas & Tóth, 2018) that have argued for more transaction-level, objective indicators, like frequency of zero and single bids, and atypical price variances, so that they can be compared in a way that capture and implicate project-level corrupt behaviors integrated within procurement systems.

Although jurisdiction-specific research can enhance the evidence base, there are inherent sampling limitations that detract from generalizability. Studies in Italy utilizing ANAC open data typically rely on datasets collected from central entities. However, this approach may produce gaps for regional and municipal procurement where the form and quality of oversight varies (Gara, Iezzi, & Siino, 2024; Autorità Nazionale Anticorruzione, n.d.). Research in Canada tends to focus on the federal context, along with the individual frameworks and institutions, with less research attention into diversity among provincial/municipal regimes operating under statutes (Treasury Board of Canada Secretariat, 2021). In the United States, much of the evidence reflects federally funded programs which have been audited by the GAO-insightful and rich in detail but may not represent diversity across state and local practices (because federal programs and states may have different procurement practices). This creates selection and surveillance bias toward entities that receive more scrutiny (U.S. Government Accountability Office, 2011; OECD, 2025).

As operationalization of corruption within procurement literature is inconsistent, this study established a definition informed by relevant extant literature and the previous definition offered. Some studies have focused solely on corruption in terms of direct bribery, or bid rigging, while also advocating broader definitions of corruption as inefficacy, bias and occlusion more broadly. Regardless of the agreed definition, inconsistent operational definitions raise challenges for cross-study comparison, especially with efforts to link varying features (and defined risks) of corruption to particular blockchain capabilities. The impact of blockchain efforts on corruption could vary across studies depending on how singularly or indirectly corruption has been suggested to be

operationalized; as an example, studies that understand corruption as simply the cost of a contract, as in the inflated price for delivery or completion, overlook other or process vulnerabilities, such as the potential for strategic use of discretional exceptions in procurement, which blockchain's encryption and immutability, verifiability or auditability could impact directly. Secondly, few studies have mapped vulnerabilities systematically through the procurement process from the design of the tender to contract implementation which limits our knowledge of where in the procurement cycle blockchain could serve as a useful intervention to influence areas of significant risk potential.

Critically, many empirical studies do not contain a clear dialogue around institutional context, which mediates corruption risk. Some quantitative studies have included political competition or media freedom as control variables, but most have not included a qualitative assessment of the culture of administration, consistency of enforcement, or clarity of regulatory codes—features that shape the process and measurement of corruption. This omission is especially pertinent to cross-country comparisons; to avoid bias examples would not include legal traditions (i.e. civil law, common law), whether federal versus unitary, or centralization of procurement. A more rigorous framework would utilize transaction-level procurement data as well as qualitative institutional diagnostics to better understand not just *where* corruption occurs, but *why* some systemic vulnerabilities continue to exist despite formal accountability measures in place to address corruption.

Confronting these methodological limitations is central to the dissertation's design. By actively questioning previously used measures and their limitations, the study is not just engaging in a descriptive synthesis but is moving toward a mechanism-oriented, logic-based comparative framework. In other words, the study is more than simply identifying typologies of corruption, but it is also focused on what the capabilities of blockchain technology are relative to various forms of corruption using an empirical, contextualized, and methodological transparent approach—filling a significant gap in the current procurement governance literature.

Across the reviewed literature, corruption in public procurement consistently emerged as lifecycle-contingent manipulation of discretion and information asymmetries, facilitated by documentary opacity and fragmented information systems. We are moving in the procurement literature from a generic prescription of transparency to mechanism–risk fit, where specific integrity controls (verifiable timestamping; commit–reveal bid submission; on-chain integrity proofs; append-only trails) align with discrete windows of opportunity available throughout the planning, publication, submission, evaluation and award stage, execution and payment stages of procurement. The feasibility and effectiveness of these procedures and processes are interceded by a mutually-supporting framework of records law, data-protection obligations, an institutional capacity, differ between Italy/EU, Canada and the United States.

This synthesis sets up the overall analytic structure that follows. Subsection 2.1.1 develops and actor typology and associated capture mechanisms; specifying who, at which level in the lifecycle, is making use of which windows of discretion. Subsection 2.2 provides a brief DLT typology that charts technical properties to the risk types listed. Subsection 2.2.2 then brings a problem-driven frame to examine implementation hazards and the other legal tensions that condition any technology agnostic approach. The logical flow of this conceptualization is set up for the next subsection, which takes the Actor–Mechanism typology from the previous section and identifies which mechanisms or blockchain controls theoretically limit whom with which actions.

2.1.1 Corruption Actor Typology and the Political Economy of Procurement Capture

Corruption in public procurement is a complex and systemically embedded process that operates through the interactions of different actors, actors who exist and act in institutional, political, and economic worlds. Corruption in procurement systems is, therefore, not an individual act of opportunism, as people engage in organized, strategic, corrupt processes carried out by networks of public officials, private sector actors, political elites, and intermediaries, existing in the same institutional context and incentives (Fazekas & Tóth, 2016; Hudon & Garzón, 2016). This means to understand the typology of different actors and the political economy at play in their functions, is vital for any serious anti-corruption process in public procurement, especially as jurisdictions like Italy, Canada, and the U.S., are complicated by legal and complex incentives from market concentration of public procurement systems that also mask vulnerability.

The primary analytical framework utilized throughout the literature is a principal agent-client paradigm and its emphasis on the relational dynamics between elected officials (the principals), bureaucrats and procurement officials (the agents), and private sector bidders or suppliers (the clients). Each class of actor has a different level of access to information, incentives, and leverage points, and thus different strategies of corruption and modes of capture (Yusof et al., 2023; Graycar, 2022). However, that model is increasingly being supplemented by network-based models that focus on coalition-building, informal intermediaries, and facilitators on the margins that help sustain corruption over the long term (Fazekas et al., 2021; Waxenecker & Prell, 2024).

Insiders in procurement agencies represent the most immediate and operationally influential actor type across all jurisdictions. They include members of the tender committee, technical evaluators, procurement clerks, and heads within an agency, who usually have discretionary power over the bid design, supplier vetting, evaluation criteria, and awarding. Insiders exploit information asymmetries and soft oversight to shape or amend procurement specifications, collude to exclude competitors who should qualify, or artificially inflate contract prices, to the personal political gain of those involved (Hudon & Garzón, 2016; Decarolis & Giorgiantonio, 2020). Often, this behavior is not rogue, but rather colluding with the tacit or direct protection of politically appointed patrons

at a higher level (Mahmalat & Maktabi, 2023). In Italy and code-aligned jurisdictions, the codes establish space for local political patronage risks; in Canada, the federal–provincial fragmentation produces differing and uneven levels of oversight; in the U.S., the diversity between states of state-controlled procurement creates uneven, heterogeneous, and varying exposure to insider discretion to these normative guidelines that can provide safety to the procurement process.

These procurement insiders typically collaborate with collusive bidders and the consultants who facilitate their collusion to accomplish bid rigging, price-fixing, and market rotation. Evidence from infrastructure procurement in Lebanon and Quebec illustrates how private contracting firms can develop long-lasting cartels that influence and control bidding, often facilitated by intermediaries like consultants and lawyers (Clark et al., 2018; Mahmalat & Maktabi, 2023). Actors that engage in collusion are exploiting dependable cycles of procurement, low competition, and discretionary contract award systems to inflate the costs of local infrastructure and continuously capture the market (Signor et al., 2022). Signals of collusion to test for would be very short bid windows, repeated configurations of bids, pre-qualification criteria that align with the eventual winner, and atypical patterns of change orders after award. The collusion networks essentially organize as closely as possible outside of the obvious, all while maintaining legal appearance, and networks can be particularly observable in settings that have limited oversight or high political interference.

Meanwhile, political actors—ministers, mayors, and parliamentary procurement committee members—utilize their influence to steer contracts towards trusted commercial allies or shell firms with familial links to themselves. This phenomenon is best articulated in the literature as state capture whereby procurement is weaponized towards political and financial gains of governing elites rather than fulfilling the public good or value (Fazekas & Tóth, 2016; Dávid-Barrett & Fazekas, 2020). In this depiction, corruption is not a simple deviation from established norms and practices but rather an outcome inherent to political economy incentives (i.e., campaign finance, party patronage, and bureaucratic propensities). Political elites are frequently implicated in state capture as they occupy both the creator of the procurement law and the person making individual contract decisions, in turn facilitating corruption both at the state level and transactional cost level (Dávid-Barrett & Fazekas, 2019; Gray, 2021).

Empirical studies increasingly underscore the significance, yet critically under-theorized, role of intermediaries and facilitators in the maintenance of procurement corruption. Intermediaries may be characterized as corrupt auditors, vendors providing IT solutions, representatives of labor unions or groups of organized criminals. Intermediaries are actors that exist in the space of semi-institutional frameworks and support, facilitate, or cover illicit transfers involved in corrupt procurement (Fazekas, Sberna, & Vannucci, 2021; Hudon & Garzón, 2016). Intermediary actors provide value in terms of lowering transaction costs associated with corruption, coverage of technical competence and expert knowledge to facilitate circumvention of detection, and continuity from electoral or administrative cycles. As an example, IT contractors who conduct customized development of procurement software or digital tendering platforms often build-in

software bugs or procedural loopholes designed to provide flagged or backdoor access for the purpose of targeted manipulation of procurement processes (Adjorlolo et al., 2025). Auditors providing oversight of finances may easily ignore inflated cost estimates or fictitious invoicing for an economic or professional compensation, during the contract term or period of assignment.

The roles of these intermediaries are diverse depending on the context, but generally involve (1) technical facilitation, addressing the manipulation of procurement platforms, audit trails, or automation of exclusion criteria upon bidding; (2) network brokering, serving as intermediaries between political decision-makers and private contractors; and (3) evasion logistics, establishing shell companies, laundering payments, or counterfeiting compliance reports (Fazekas et al., 2021; Lyra et al., 2022). Theoretical models such as entrepreneurial coalition building (Hudon & Garzón, 2016) and extra-legal governance (Fazekas, Sberna, & Vannucci, 2021) illustrate how these actors create nimble alliances that adjust to regulatory changes. These coalitions, frequently organized around core decision-makers (including political elites and procurement officials), will have a network of service providers and intermediaries who collaborate to evoke the addition of time and secrecy to corruption schemes.

The literature similarly highlights the ways that union intermediaries and public sector insiders cooperate in situations of labor representation and procurement execution. Unions or staff associations may be a gatekeeper to important procurement committees or technical working groups and require side-payments or job placements, or other forms of cooperation or silence (Fazekas & Kocsis, 2017; Dewantara & Sukarmi, 2024). Such dynamics are observed in labor-intensive contexts such as public works or health care procurement, whereby negotiation over labor interest is included in corrupt negotiations.

In all categories of actors, the rationales for participation in corruption in procurement, blend together those rooted in instrumental rationality, political survival and opportunism for organizations. In government procurement, personal gain is usually the most proximate explanation, usually in the form of bribes, kickbacks or illicit accumulation of economic assets and benefits (Rustiarini et al., 2019a; Misran, 2024). However, structural rationales such as campaign finance earmarks, loyalty to political machines and continuing organizational continuity in non-transparent bureaucracies are now being considered as more central to why corruption in procurement exists in some contexts (Dávid-Barrett & Fazekas, 2020; Fazekas, Cingolani, & Tóth, 2016). In some contexts, public officials rationalize corrupt behaviors as a strategy for mismanaging a budget deficit, rewarding a employee's loyalty, or navigating competing administrative agendas (Graycar, 2022; Rustiarini et al., 2019b).

At the network level, the mechanisms of procurement capture are maintained not only by individual interests but also by the institutional arrangements that lower the cost of corrupt behavior but also lower the risk of being caught. Limited oversight agency, fragmented bureaucratic mandates, insufficient transparency of bidding data, and underfunded anti-corruption agencies create an environment where corrupt practices can become entrenched (Bauhr et al.,

2020; Adesola et al., 2024). Even when anti-corruption measures are put in place (e.g., audit reforms, e-procurement systems, and conflict of interest disclosures), literature consistently highlights how actors simply adjust, either by changing their forms of corruption, or embedding new forms of corruption into new systems (Fazekas & Wachs, 2020; Avdasheva et al., 2025).

A significant aspect of the literature relates to the capacity of corruption networks to adapt to regulatory shift and anti-corruption reforms. In many situations, these corrupt procurement networks do not disband, but rather respond in other ways to increased scrutiny—through changes in mode of operation, personnel, or by taking advantage of new loopholes in processes (Fazekas & Wachs, 2020; Gnaldi & del Sarto, 2024). This adaptive capacity is well documented in the literature on digital procurement systems—where reforms such as e-tendering, online contract disclosure or algorithmic scoring, are originally introduced to mitigate discretion and inequality of information. However, studies reveal ways for corrupt actors, specifically those privies to advanced technical know-how, to adapt procurement processes to contain new manipulations—such as automated exclusion of disfavored bids, pre-programmed specifications or changing time stamps on bids (Adjorlolo et al., 2025; Avdasheva et al., 2025).

This phenomenon is what Fazekas, Sberna, and Vannucci (2021) refer to in their discussion about the extra-legal governance of corruption, whereby corrupt actors mimic aspects of legal institutional order (stability, continuity, specialization, etc.) within an informal governance network that operates in parallel with prescribed formal procurement rules. In these contexts, institutional weaknesses are not simply used as levers but integrated into the structure of corruption. Loose enforcement of conflict-of-interest legislation, vague tenders, or delayed audits become structural facilitating mechanisms, rather than administrative failures (Decarolis & Giorgiantonio, 2020; Bauhr et al., 2020). These institutional weaknesses become normalized entry points whereby the capture of procurement is institutionalized, especially when auditing and oversight institutions lack independent operational capability or are subject to political interference.

At a macro level, this increasing sophistication comes together in the literature as state capture: a form of systemic corruption where procurement institutions themselves are actually used to serve the entrenched political–business relationships. In these situations, it is no longer that procurement systems can be manipulated; procurement systems would be intentionally constructed or structured to prey on the system (Fazekas & Tóth, 2016; Dávid-Barrett & Fazekas, 2020). Their empirical work in Hungary, Mexico, and Italy clearly demonstrates that public contracts are awarded to a tight-knit, politically connected group of firms which is quite evident in the manner of contracting, where firms go back to the same firms over and over again, using opaque mechanisms, repeat bidding, and legal exemptions (Fazekas, Cingolani, & Tóth, 2016; Falcón-Cortés et al., 2021).

Although the manner or model of state capture is obvious in multiple jurisdictions, the modality of capture looks quite different based on national procurement architecture and administrative cultures. For instance, in civil law systems, such as Italy, complex layers of regulation and

centralized bodies of oversight may be evaded through local political patronage and exemption under emergency procurement (Gnaldi & del Sarto, 2024). Conversely, in a federal system like Canada, the opportunity for capture may occur through a provincial-level procurement regime that lacks intergovernmental coordination and oversight, thereby providing a political actor with the opportunity to dictate a contract towards a favored firm without sufficient federal scrutiny (Khamitov, Knox, & Junusbekova, 2023). In the United States, fragmentation of procurement throughout state, municipal, and federal agencies has created a patchwork of vulnerabilities, especially in areas such as infrastructure and defense contracting where enormous budgets are involved yet there is minimal centralized focus or oversight (Signor, Love, & Ika, 2022; Gray, 2021).

Capture, irrespective of jurisdiction, usually arises through a combination of legal manipulation mechanisms (e.g., regulatory cloudy language, exceptions to competitive bidding), institutional inertia (e.g., poorly-resourced watchdog organizations, outdated oversight processes), and co-optation of accountability systems (e.g., politicized audit offices, revolving-door practices for hiring). When these patterns are sustained over time, procurement corruption becomes deeply embedded in the system, rather than being a one-off failure, and actions to curb it go beyond an audit and enforcement approach (Thomann et al., 2025; Dávid-Barrett & Fazekas, 2019).

In addition to structural and institutional forms, recent literature has also focused on micro-level factors in an individual's choice to act corruptively - psychological motivations, behavioral rationalizations, and the organizational culture that fosters unethical behavior in the context of procuring goods and services. Although these factors were historically overlooked, contemporary literature has started to show that corruption can survive not only through opportunity, but also through moral disengagement, social evidence, and justificatory cognitive processes (Rustiarini et al., 2019b; Misran, 2024).

The fraud triangle and fraud diamond frameworks—concepts regularly used in public administration research—locate pressure, opportunity, rationalization, and capability as the four elements that aid corrupt acts. Specifically, Rustiarini et al. (2019b) conducted qualitative interviews with Indonesian procurement officials and find opportunity (weak controls and low likelihood of being caught) as a necessary but not sufficient condition. It was often the rationalization dimension, seeing bribery as compensation for "helping facilitate efficiency," that would trigger a breach. The study noted that peer norms and organizational acquiescence were also important enabling factors, especially in cases of a rotational procurement role and when it was unclear who was being held accountable. These behavioral dynamics are always negotiated with institutional incentives to produce decisions about how and when to employ corruption mechanisms throughout the procurement lifecycle.

Misran (2024) provides further empirical depth to the psychological dimension by analyzing how individual morality, arrogance, and greed influence the risk of procurement fraud in South Kalimantan’s local governments. The study employed a structured survey methodology across 240

civil servants and found significant positive correlations between arrogance scores and rule-breaking tendencies in procurement settings. Interestingly, respondents who scored high on moral reasoning but operated in low-accountability environments were still likely to compromise ethical behavior when surrounded by informal pressures or promises of protection. This reinforces the notion that institutional setting and psychological traits are deeply intertwined, and that internal moral frameworks can be overridden by external incentives or threats. In this model, these micro-level drivers act as moderators of the mechanism–risk fit whether timestamping, commit–reveal, or audit-trail controls actually change behavior within a given agency culture.

According to Fauziah and Marpaung (2024), in their examination of conflict of interest in Indonesian public procurement, it is pointed out how role confusion and competing loyalties lead to further degradation in judgment within ethical decision-making. Investigating the case file of public officials undertaking institutional duties of procurement and political campaign simultaneously, they showed how role overlap within institutions creates a dynamic of cognitive dissonance within actors who reconcile that dissonance through informal loyalties over formal modes of conduct. The authors conclude that current training protocols along with disclosures of conflict of interest will not suffice for counteracting organizational issue, particularly with an organizational culture that upholds hierarchy as a standard over substantive accountability.

Graycar (2022) presents a more conceptual approach to the issue by stating that you cannot resolve procurement corruption through external monitoring mechanisms. Rather, after examining multiple international case studies, he points to the role of an organizational "tone at the top" and ethical leadership in shaping staff behavior. He further criticizes the use and reliance on traditional principal-agent models, which often overemphasize economic rationality, and instead proposes a hybrid behavioral-institutional framework whereby systemic incentives and a person's ethical disposition work in unison to be co-determinant in behavior. Importantly, Graycar notes that having ambiguity in rules and using discretionary decision-making, increases the potential for staff to rationalize corrupt behavior, even if the staff member has good intentions.

While these studies differ distinctly in their methodological approaches, and they may appear on the surface to be disparate, they point to a central conclusion: procurement corruption cannot be simply explained solely through failings of institutions or failures in enforcement capabilities. Rather, the internal cognitive, cultural, and moral processes that operate within organizations/ agencies, arising from both individual and organizational behavioral signals creates an important and different consideration. The implication for anti-corruption policy for government and indeed the wider policy arena, is that reform needs to consider procedural safeguards and oversight capabilities and behavioral training and ethical strengthening, as well as mechanisms for changing the culture of procurement units, at the same time.

Collusive bidders and strategic consultants represent an actor group at the crossroads of the complex interactions between the competitive marketplace and the various procurement process. These private sector actors collectively engage in collusion, often as part of a cartel or informal

network, to maximize the ability to exploit the weaknesses of a competitive bidding model, and, as a result, secure multiple and inflated awards. While collusion is frequently thought of simply as price-fixing or bid rotation, recent literature highlights the much wider possibilities of market manipulation and strategic entry deterrence that these types of actors use, and particularly with respect to the procurement of infrastructure and public service delivery (Clark et al., 2018; Chiappinelli, 2016).

Clark et al. (2018) focused on procurement related corruption in Quebec, Canada by using forensic evidence from a provincial inquiry into procurement revealed how contractors, in collaboration with corrupt government bureaucrats, developed a wholesale, systematic scheme of bid suppression. Winning bidders were pre-arranged in exchange for kickbacks and other rivals submitted deliberately inflated price quotes or didn't bid. The scheme utilized non-compete pacts and market division agreements implemented through social pressure or sanctions through cartels. The main takeaway from this study was that entry deterrence mechanisms were deliberately embedded into the procurement cycles, such as carving away precious bid time, insider knowledge or arbitrary pre-qualification criteria that only the known participants would satisfy.

Chiappinelli (2016) provides a complementary theoretical examination of how political connections and legal ambiguities reinforce collusion incentives during the execution phase of public contracts. As the analysis uses microeconomics and game-theoretical models, it shows how obtaining the contract creates moral hazard and asymmetric enforcement opportunities for colluding firms. The exploitable incentives manifest themselves to allow colluding firms to mismanage contract resources or overcharge the contract with almost no chance of legal penalties. These incentives are most pronounced when renegotiation is easy, there are multiple commodities to be considered by different supervisors, and political patrons provide a buffer for the provider's reputation. Chiappinelli examined a different aspect, with the findings showing collusion acts in the bidding process, with a second layer of corruption occurring after award of the contract. The study identified consultants as a bridged entity between contractors and procurement personnel as a clear example of material benefit provided by a corruption system.

More granularity on the formal characteristics shared heretofore, with Lyra et. al. (2021) using network analysis of procurement data in Brazilian municipalities to examine firm-firm co-bids, their analysis complements those of both Chiappinelli and Manunza as they documented that, for several tenders, there were organizationally and/or geographically focused coordinated bidding strategies. The study provided evidence of firm clusters that would bid on the same tender’s multiple times providing characteristics as either tacit or explicit coordination. Clusters on firms were geographically close together, with success in awarding of contracts well beyond that of firms with which they have no affiliation. Thus, the implication of their work is that while single examples do not provide distinct proof of collusion, the analyses of statistical characteristics similar over time and with bidding consortia reflect an organized bid capture strategy. The study illustrates the role social have network mapping may have to act as monitors to provide a early

warning system to monitor anti-collusion processes, this is relevant in contexts where there are significant challenges to obtain legally admissible evidence.

The studies illustrate that colluding actors employ a two-pronged strategy: (1) restraining competition at bid time through informal coordination or procedural manipulation, and (2) extracting rents during contract execution through renegotiation, delay or technical complexity. Consultants, attorneys and engineering auditors are often implicated as knowledge brokers who have sufficient understanding of the procurement system to assist firms in exploiting known vulnerabilities. These facilitators are rewarded not directly through contract awards, but through side payments, sub-contracting, or revolving door employment opportunities (Lyra et al., 2022).

The implications for procurement integrity are far-reaching. Collusion among private actors impedes market efficiency, increases public expenditure, and provides for path dependency in procurement relationships. Once established, these networks tend operate to exclude entrants, stifle innovation and diminish price competitiveness, particularly in sectors where contract size and technical specifications create high entry barriers (Chiappinelli, 2016; Clark et al., 2018). Furthermore, the concealment techniques used by colluding actors—legal cartels, consultant intermediaries and bid bundling—will commonly be difficult to detect using traditional audit techniques and will, therefore, require more companionate data analytics and regulatory reform.

The procurement corruption architecture is increasingly reliant on a class of actors who work to facilitate illicit transactions outside the scope of formal or institutional boundaries: peripheral and shadow actors. These peripheral and shadow actors include types of organizations like shell companies, front companies linked to family members, politically exposed persons operating through intermediaries, and even organized crime syndicates. The primary role of these peripheral and shadow actors is to mask the identity of the true beneficiaries, facilitate illicit flows of money, and protect central actors such as procurement agents, and their political benefactors, from exposure or liability (Fazekas, Sberna, & Vannucci, 2021; Palidauskaitė & Ereminaitė, 2010).

The research conducted by Fazekas et al. (2021) implicates the emergence of extra-legal governance structures in the Italian public procurement context whereby organized criminal actors facilitate transactions and enforce order in procurement networks. Furthermore, these actors often do not limit their services to protection or laundering; they may either directly facilitate collusion between bidding firms, provide bribes to participant insiders or manage front companies to submit bids or run the subcontracting layer. The researchers trace the pattern of transactions occurring in public tenders and delineate how these groups decrease the 'corruption transaction costs' by deformalizing risk and uncertainty for primary decision-makers and actors in the specific region through which they operate - often a region with limited and/or compromised law enforcement capacity.

The second research study included in the review is Palidauskaitė and Ereminaitė (2010), which outlines a definitional and case study on shell companies as de facto vehicles of corruption in public procurement. In their prescriptions on the case of Eastern European procurement fraud, the

study investigates the shell firm as not simply a legal fiction but an institutional tool, enabling corrupt networks to simulate competitive tendering, divert funds from the public procurement layer to corrupt network political or personal allies, or conceal ownership by layering nominee directors in the shell firms' and ultimately in the bidding process. Shell companies generally exhibit characteristics of being short-term, lack any operational capacity or physical presence, and typically are registered by third parties and intermediaries (e.g. accountants, legal services). The authors argue that procurement laws that address conflict of interest do not generally account for these proxy structures, particularly when ownership registries are fragmented and/or opaque.

Research on Guatemala suggests that procurement corruption generally functions in adaptive networks rather than stable cartels. A longitudinal study of local construction contracts (2012–2020) shows collusion and spending concentration ebbing and flowing alongside electoral cycles and anti-corruption crackdowns, but instead of returning to dormancy during spikes in oversight, actors disrupt patterns temporarily as they reconfigure (Waxenecker & Prell, 2024). Signals of observable affiliation that usually accompany such coordination include shared business addresses, recent changes in corporate structure, and connections on the basis of kinship or previous political status. All are confirmatory risk indicators on the procurement literature (Gnaldi & Del Sarto, 2024; Amore & Bennedsen, 2013). Relatedly, constellations of shell companies can also be mapped through connections based on management/ownership and contracting data, and stable supplier clusters emerge in studies of public tenders (Nicolás-Carlock & Luna-Pla, 2024). While I do not find a lot of evidence for the precise claim about shells controlled by PEP prioritizing Italian emergency awards, I stick with a narrower formulation here and use amendments as a measure of red flags during the emergency period rather than definitive award decisions (Gnaldi & Del Sarto, 2024).

Often, these peripheral actors include family members of political elites or senior bureaucrats similarly inserted as shareholders, consultants, or subcontractors in successful firms. By inserting family members in such contracts, key actors in procurement corruption can obfuscate ownership structures, avoid accountability, acquire profits indirectly, and engage in cover-ups plausible in denial when resolving procurement accusations. For example, Fauziah and Marpaung (2024) found in jurisdictions under weak asset disclosure regimes that a common way to move contract flows to family or personal connections was to insert members into ownership structures, while still fulfilling strict legal eligibility requirements. Likewise, in their analysis of Italian procurement during emergency times, Gnaldi and del Sarto (2024) described how contracts were disproportionately awarded to shell entities owned or controlled by politically exposed persons through legal exceptions or fast-track processes.

Corruption actors on the periphery function as modular, reconfigurable entities versus a fixed hierarchy and are uniquely positioned to adapt networks to regulatory shocks, political cycles, and investigations with minimum loss of capacity—one of the reasons that blacklist and registration controls do not work as well as prescribed (Fazekas et al., 2021; Nicolás-Carlock & Luna-Pla, 2024; Waxenecker & Prell, 2024). Disruptive success targets functions, not legal wrappers, with

enforceable conflict-of-interest/debarment rules, beneficial-ownership transparency and verification, and risk analytics based on networks. Indicative observables include opaque or rapidly changing ownership before award; clusters of bidders sharing contacts or directors; agglomerations of firms that dissolve immediately prior to or following performance; and repeated subcontracting to firms with connections to PEPs. Use as screens considering jurisdiction-specific evidentiary and data-protection restrictions.

Despite the fact that the typology of actors and behaviors in procurement corruption is being documented well, it is often the institutional milieu that determines the level of corrupt behavior and longevity. Across contexts and governance theories, the literature has come to an important conclusion: these institutional weaknesses like fragmented oversight, unclear legal frameworks, and procedural inconsistency do not merely foster corruption; they are central to procurement capture (Bauhr et al., 2020; Ferwerda, Deleanu, & Unger, 2016). These weaknesses can be actively exploited through conduct learned by manipulating weak processes, pack co-opting an accountability body to weaken their agency and/or deliberately undermining procedural completeness; all of which means that actors with only moderate resources can cause systemic degradation of competitive integrity.

Bauhr et al. (2020) set out to assess procurement transparency reforms across EU member states, and if simply increasing the transparency of tender document and award decisions improved competitiveness in social democracy. They found, ultimately, that while increasing openness of these spaces improved overall competitiveness, increasing transparency alone is not sufficient in institutional environments lacking enforcement and civic engagement. The study specifically notes that many procurement portals that were introduced under the auspices of anti-corruption initiatives displaced corruption and opacity to actors within other phases of the procurement cycle - like technical evaluation or renegotiation - when vulnerable exploiters were at another phase. They conclude by arguing for a systematic approach where transparency is combined by institutional independence and whistleblower support, or to simply be cautious of providing a mistaken sense of integrity through independent interventions isolated from complaints or assessing integrity on any evidence.

Ferwerda et al. (2016), employing a typological categorization of oversight institutions in OECD and non-OECD countries, uncover stark variation in their capacity and organization. The authors identify three main failure modes: (1) jurisdictional overlapping, in which several agencies have overlapping jurisdiction and work without coordination; (2) procedural complexity, which generates loopholes and processing delays; and (3) resource asymmetry, in which the procurement system is better financed and technically able than its anti-corruption or audit institutions for the monitoring of the procurement system. In these environments, even the most carefully drafted procurement regulations can fall prey to institutional inertia, which renders the regulations ineffective.

The complexities associated with these institutional failings are further illustrated in the work of Gray (2021), who undertook a political ethnography of the dynamics involved in procurement public services in South Africa. Gray shows that, in addition to the legal and procedural failures, there is a culture of "strategic compliance" within procurement offices. Here, employees are legally required to comply with procurement rules, while also working informally to undermine compliance through selective enforcement and administrative discretion. The actions of procurement staff are justified through survival narrative style of meaning-making claims, such as that they must "work around the system" to fulfil politically established quotas of service delivery. The research further highlights that formalized standards are not an indicator of actual practice, nor should they solely be pitted against institutions; rather, a norm of institutional living, negotiation and dynamic arrangements must be analyzed in understanding institutional procedures.

In a study of domestic legal systems in Eastern Europe, examined by Rogleva (2020), the author points out that the design of such procurement law may itself be an enabler of corruption. Laws that establish procurement frameworks often include broad exceptions, ambiguous eligibility criteria, or generally set discretionary thresholds for grants of direct awards, thus providing a legal defense for capturing or manipulating a procurement framework. In his comparative case, Rogleva indicates that emergency procurement clauses, which were established to support unplanned emergencies, were often expeditiously approved for non-emergency expenditures, thus avoiding open competition. The results of this study suggest that legal design flaws, often undone by or unintended within design frameworks, are often used, both by public and private actors, to escape the accountability those institutions were established to provide.

Gillespie (2021) offers a normative perspective, emphasizing that accountability in public procurement systems needs to not only consider ways to promote transparency and oversight, but also ways to ensure public representation. His research critiques the technocratic design of anti-corruption instruments that measure compliance metrics rather than ethical imperatives, or citizen engagement. Gillespie argues for a model of public interest governance, where actors in the regulatory agency, civil society organizations, and media memberships co-produce accountability. This challenges the dominant narrative that procurement integrity can only be established through surveillance and rule-based sanctions, and emphasizes the importance of inclusive legitimacy.

Both articles demonstrate that we cannot treat institutional weaknesses as residuals of underdevelopment but as embedded, structured, organized, and politically maintained behavior. They provide the frame in which actor strategies, collusive or intermediary-based, or politically orchestrated, can act on their chances of being exposed, or subsequent punishment. This means that diminishing procurement corruption would involve two strategies: (1) to strengthen institutional coherence and insulate any due diligence type of accountability from political aspirations and political authorities; and (2) re-enforce the behavioral and network level strategies.

The motivation of actors is another area to explore in order to understand the resilience and adaptability of corruption, which can span an array of motivations, from a self-interest in material

acquisitions and political utility to organizational necessities. Though the most visible motivation continues to be personal enrichment, recent studies have revealed that corrupt behavior can often be driven by multi-level incentives, including pressure to deliver political patronage, provide campaign finance, and ensure bureaucratic continuity in hostile institutional contexts (Adesola et al., 2024; Dávid-Barrett & Fazekas, 2020; Khamitov, Knox, & Junusbekova, 2023).

Adesola et al. (2024), who examined corruption dynamics across African public institutions, observed that for many mid-level procurement officials, corruption was not merely a route to personal enrichment, but a strategy of professional survival. In environments characterized by informal quotas, political interference, and vague promotion criteria, officials who resisted their requests for payment—and especially officials who resisted them out of their formal, public duty—found themselves marginalized or reassigned. In contrast, officials who complied—whether actively or passively—found themselves rewarded with access to high-profile tenders and/or better assignments. This logic of survival blurs the line between coercion and complicity, further suggesting how organizational incentives can deliberately precipitate rule-bending behavior.

Political motivations are also crucial. Dávid-Barrett and Fazekas (2020) demonstrate through a large-scale cross-national study that procurement often serves as a vehicle for political parties and elected officials to direct public resources to select firms, financiers, or geographical constituencies. Their data capture relations of systemic contract award patterns that follow election cycles, in which those firms with some association with the elected party status receive overwhelming quantities of awards—in particularly close election contexts. The research challenges the presumption that procurement corruption is solely opportunistic, instead demonstrating that many times the corruption is strategically intertwined and incorporated into political finance and patronage systems.

Khamitov et al. (2023), who examined procurement corruption in Kazakhstan, contextualized corruption within the wider dynamics between the state and society. They found that for politically unstable regimes, procurement systems function as arenas for bargaining among elites, who distribute contracts not to achieve efficiency, but to maximize loyalty and minimize defection. Under these circumstances, procurement decisions serve both symbolic and material purposes - signaling an individual's inclusion in networks of power and redistributing rents to politically significant actors. This strategic use of corruption to achieve political cohesion is consistent with observations in both the post-Soviet and Latin American contexts, suggesting, despite regional variations in the manifestation of corruption, a convergence of logic. Lyra et al. (2022), through a systematic review on collusion and fraud detection, indirectly speak to motivation by demonstrating that corrupt firms often make substantial investments in learning the methods used to manipulate procurement systems. The investment methods included hiring consultants who specialize in public tendering, creating internal compliance departments designed to mimic legitimacy and implementing front firms with limited liability to diversify exposure. This behavior suggests a rational assessment, where expected benefits associated with procurement capture outweigh mitigation costs in the event of detection. It also reflects the intersection of profit-

maximizing motivation, regulatory arbitraging and legal engineering, particularly in instances of lackadaisical enforcement of regulatory sanctions.

The convergence of these motivations with institutional fragility is important. As Rogleva (2020) and Gray (2021) argued, corrupt actors do not act in a "vacuum of motivation"; rather, their motivations for committing acts of fraud or colluding or manipulating procedures will be predicated on their sense of risk, opportunity, and legitimacy. When institutions are opaque, legal consequences are negligible, and leadership communicates tolerance for corruption, even peripheral actors will have a vested interest in participating. On the other hand, when there is strong oversight, sanctions are credible, and ethical leadership is present, motivation for these actors will be significantly reduced.

It is also important to keep in mind that motivations are not mutually exclusive. A "procurement director" who was appointed politically, for example, may have personal motivations to enrich themselves to satisfy political obligations but also the need to be cognizant in a fragile bureaucracy of protecting their own career. The intersection of these motivations creates a mutually reinforcing ecology of corruption, where procurement has become determined by private utility against political expediency, versus normalizing public value.

A coherent taxonomy of corruption mechanisms in public procurement, uniting the literature on actor roles, motivations, and institutional contexts, comes to the fore here. This encompasses mechanisms across a continuum from overt methods including bid-rigging and bribery, to more subtle mechanisms like procedural sabotage or revolving-door recruitment. These behaviors should not be thought of as random acts, but rather tactics selected by specific arrangements of actors, in response to political incentives and regulatory failures (Patar et al., 2024; Sharma, Sengupta, & Panja, 2019; Falcón-Cortés et al., 2021.). The most documented mechanism is bid-rigging were contractors conspired to pre-determine the winner of contracts. This is typically undertaken via a cartel formed of private firms, with tacit approval of, or direct collusion from, those inside the procurement process. Sharma et al. (2019) systematically mapped corruption risks in the Indian public procurement process and identified forms of collusion such as repeated patterns of bidding, exclusionary bid criteria and synchronized bidding, as indicators of collusion. Moreover, bid-rigging was made possible via insiders abusing the system, where they selectively arranged timelines, disqualified rival firms and such. Bid-rigging, therefore, can be inferred as an operation reliant on networks of influence involving market actors and insiders.

Cost-padding and over-invoicing is similarly a technique typically implemented post-award. Patar et al., (2024) in their research of procurement fraud in Central Lombok, Indonesia, demonstrated contract values are routinely inflated through fictitious expenses, ‘ghost’ subcontractors, and inflated performance metrics. These inflated contracts are then shared with political sponsors, consultants and technical evaluators. The authors implied officials carried out the practice using accountability systems for performance as a veil, accepting minimum viable outputs for budgetary discrepancies, relying on bureaucratic complexity and emergency procurement rules. This

demonstrates the use of compliance protocols for dual purposes with respect to concealing capture of public resources.

A third form of procurement fraud is regulating procurement procedures whereby the actors deliberately exploit the ambiguity within the regulations to limit competition and steer contract awards toward a specified contractor. Falcón-Cortés et al. (2021), provide examples in their examination of procurement in Mexico before and after a government transition. Agencies would sometimes invoke urgency in order to wasteful competitive bidding, or develop eligibility criteria to match the firm they had designated to receive procurement work. In some cases, entire procurement procedures were cancelled, and majority of public announcements re-issued under conditions that favored politically connected suppliers. This embodies a common political instrumentalization of procurement law, whereby legal exemptions around procurement are re-interpreted strategic routes of capture.

Simultaneously, bribery and gift-giving persist as transaction mechanisms to alleviate administrative holdups or ensure good scores during analysis. In highly institutionalized contexts, such activities are often coded as "consulting fees" or other forms, such as campaign contributions, legal retainers, or employment opportunities. Gnaldi and del Sarto (2024) provide evidence of how such actions are normalized in the setting of emergency contracts, where discretion is high, and documentation is nearly absent. These are not just economic transactions but also relational transactions that serve to solidify loyalty networks and long-term reciprocity.

In more sophisticated ways of hiding, the use of shell companies and front organizations is typically linked to political elites through family members or transparent ownership structures. As mentioned above, these entities are purposely created to simulate competition, albeit with layered owners that absorb the risk. These entities are typically used for bid bundling, in which several separate bids originate from a single network despite the appearance of independence. Usually, these entities will be dissolved shortly after the execution of the contract, creating a temporary trace of accountability. Lyra et al. (2022) framed this tactic as one of several interchangeable legal entities in a larger modular structure of corruption; although the legal entity is absent, they remain a part of a network.

In conclusion, corruption in public procurement not only takes on various forms, but it is also strategically organized: different actor combinations (e.g., collusive bidders, insider public officials or political elites, IT vendors) gravitate to mechanisms that are most compatible with their access, knowledge or expertise and risk tolerance. These mechanisms are used flexibly, sometimes in combination, and change over time with oversight situations, legal reforms or state changes. Therefore, anti-corruption interventions need to be situationally specific to these constellations and not simply the acts. Corruption mechanisms are shaped by relational dynamics and institutional design, not just individual intention.

Table 1.Table 2.1.1. Mechanism–Control Mapping Across the Public Procurement Lifecycle: Legal Prerequisites and Auditable Outputs (Italy/EU, Canada, U.S.)

Procurement Stage	Corruption Mechanism (Risk)	DLT Control (Design Choice)	Legal/Regulatory Prerequisites (Rule/Evidence Hook)	Auditable Output
Pre-tender planning	Inflated scope, tailored specifications, opaque approvals, and unrecorded changes to the needs assessment.	Version-controlled repository (append-only hashing), role-based e-signatures, optional public hash anchoring	EU/IT: BDNCP/PAD for official publication/records (D.Lgs. 36/2023; ANAC 263/2023); GDPR: keep PII off-chain, store on-chain commitments; Evidence/signatures: eIDAS (EU), ESIGN–UETA (US), PIPEDA + Secure E-Signature Regs + Canada Evidence Act (CA).	Versioned dossier with sign-offs, hashed draft history, exportable signed minutes, and a brief verification guide with hash receipts
Tender publication	Late/altered notices, selective disclosure, unpublished amendments limiting competition.	Certified publication via PAD/BDNCP (IT/EU), Canada Buys (CA), or SAM.gov (US); notice hash anchored to a public chain with authoritative timestamp.	PAD/BDNCP receipts (D.Lgs. 36/2023; ANAC); transparency: FOIA (US), ATIA (CA); evidence: FRE 901/902(13)/803(6) (US), Canada Evidence Act ss. 31.1–31.8 (CA).	Publication receipt, cryptographic timestamp, and a notarized PDF+JSON export with notice details and OJ/POE IDs
Bid submission	Bid tampering/deadline gaming; unequal access; premature decryption of sealed bids.	Use a sealed-bid **commit–reveal** protocol with cryptographic time-stamps, threshold decryption at bid opening, and tamper-evident submission logs.	Integrity: eIDAS/ESIGN–UETA recognize timestamp/commit for submission and signatures; Canada Evidence Act ss. 31.1–31.8 (electronic records); EU Data Act requires smart-contract logging/interruptibility.	Sealed-bid receipt (hash and signature), timestamped submission, and an opening transcript recording key release and bid order.

Evaluation & award	Score manipulation/favoritism; off-record overrides of criteria/weights.	Deterministic scoring pipeline (on-chain or verifiably logged off-chain); human-in-the-loop review; signed decision memorandum; challenge-window logging.	EU: Data Act Art. 36; eIDAS. US: FRE 901/902(13)/803(6). CA: Canada Evidence Act (electronic records).	Deterministic scoring log, signed decision memo, edit history (user IDs), and challenge-window log.
Contract execution	Gold-plating, non-delivery, change-order abuse to divert value post-award.	Milestone-based proofs (deliverable hashes, inspection attestations, oracle evidence for geo/time/photo), immutable change-order ledger, dual-signature approvals.	Trust services: eIDAS (EU); ESIGN–UETA (US); PIPEDA and Secure Electronic Signature Regulations (CA). Evidence packaging: treat the ledger as an integrity layer (off-chain data, on-chain commitments).	Milestone evidence (deliverable hashes and inspection attestations), an immutable change-order record, and dual-signature approvals.
Payment & close-out	Fictitious invoices, duplicate payments, concealed late payments, and mismatched deliverables.	Three-way-match (PO–GRN–invoice) with on-chain proofs; retention-aware evidence packaging; disclosure-ready export bundles.	US: FAR 4.5, FOIA; FRE 901/902(13)/803(6). CA: ATIA; Canada Evidence Act ss. 31.1–31.8. EU/IT: BDNCP/PAD. Evidence: integrity-layer packaging.	Three-way-match proof, signed payment authorization, immutable payment record referencing retention, and a FOIA/ATIA-ready redaction/export bundle.

Notes :(legal/evidence hooks)

Italy/EU publication and records. BDNCP/PAD are the statutory channels under D.Lgs. 36/2023 and ANAC Delibera 263/2023 (pubblicità legale).

Data protection. GDPR's storage-limitation rule bars indefinite on-chain personal data; use off-chain repositories with on-chain cryptographic commitments.

EU trust services. eIDAS gives qualified e-signatures legal effect; identity assurance is provided by qualified trust services (EUDI Wallet emerging).

Canada. PIPEDA, the Secure Electronic Signature Regulations, and the Canada Evidence Act (ss. 31.1–31.8) govern electronic records/signatures; ATIA sets disclosure requirements.

United States. FOIA; FAR Subpart 4.5; FRE 901, 902(13), 803(6); and ESIGN/UETA ensure functional equivalence for electronic signatures and records.
Evidence packaging. Treat the ledger as an integrity layer: keep identifiable data off-chain, store hashes/receipts on-chain, and provide signed export bundles for auditors/courts.
EU Data Act. Article 36 mandates logging and safe termination/interruptibility for smart-contract operations used in procurement.

Table 2.1.1 focuses on enhancing construct validity by explicitly linking each corruption mechanism to its legally defined function for its procurement stage, which could be publication, submission, evaluation/award, execution, or payment - in a way that the proposed DLT control is not just technical, but in normative terms it must apply just by virtue of conduct throughout the procurement lifecycle. Further, the column "auditable outputs" translates abstract constructs into audit-able artifacts. For example, a sealed bid translated to an on-chain, timestamped commitment, along with a verifiable bid opening transcript and a de-identified bid (the contracted amount), preserves the taxonomic level of a sealed bid. Our revisions are complementary to an Italian codified publication/platform regime (D.Lgs. 36/2023; ANAC Delibera 263/2023) (Governo della Repubblica Italiana, 2023; Autorità Nazionale Anticorruzione, 2023). Architecturally, we treat the ledger as an integrity layer. Where a public procurement process requires personally identifiable information or sensitive data, that data remains off-chain in order to meet their storage-limitation duties and accuracy duties under the GDPR but can point back to on-chain records, but the on-chain meritorious records codify the cryptographic commitments of the disclosure along with the metadata of the receipt, which is necessary to matter because they equate to evidence (sending the message about their surrounding circumstances) and allow for the lawful rectification or any required changes without having to re-enter or rewrite the provenance of an object in the ledger system (European Parliament & Council of the European Union, 2016). Statutory portals - PAD/BDNCP (Italy/EU), SAM.gov (United States), CanadaBuys (Canada) - will be the authoritative locus of publication for these statutory duties of disclosure. That said, some or all of these portals, based on their designations, may and can use public chain registry to create an independent timestamped indexing resolvable level - inked to the compliance of public procurement regimes - that creates an additional factor of resistance to collusion (i.e., added resource to time and transparency), while maintaining a live connection back to disclosure regimes like FOIA/ATIA/whatever is legally prohibited. (Governo della Repubblica Italian, 2023; U.S. General Services Administration, 2023; Government of Canada, 1985/2025).In the competitive stages, a commit-reveal scheme with time-stamped cryptography maintains bid secrecy until the submission deadline and provides self-authenticating process logs that would qualify as having evidentiary authentication under the Federal Rules of Evidence, Rules 901/902(13), as well as under the business-records exception (803(6)), as allowed by Canada Evidence Act, with the same effect of the presumptive ability to allow for electronic records. This is known by the functional equivalency of signatures under eIDAS in the EU and ESIGN/UETA in the US (United States

Courts, 2017/2019; Government of Canada, 1985/2024; European Parliament & Council of the European Union, 2014; United States Congress, 2000; Uniform Law Commission, 1999). Where there is an automated aspect related to evaluation (not evaluation of human decisions), Article 36 (Transparency) of the EU Data Act specifies logging, safe termination, and interpretability of the automated evaluation. Thus, the design preserves human-in-the-loop authority and provides a deterministic log with signed memorandum decisions for administrative-law review (European Parliament & Council of the European Union, 2023). For binding acts (related to identity assurance), qualified trust-services, as specified in eIDAS and assurance levels specified by NIST SP 800-63-3, provide the legal basis for identity assurance required for authenticity. Export bundles would have the signature validation material for independent verification (European Parliament & Council of the European Union, 2014; National Institute of Standards and Technology, 2017). Evidence packaging entails the record, a manifest in JSON of hashes/timestamps, and signature certificates, allowing for independent verifiable reproducibility, while fulfilling access/redaction duties (United States Courts, 2017/2019).

Research on corruption in the field of public procurement has reached a greater level of sophistication in understanding the embeddedness of corruption in the larger institutional and political economic context. It is clear that corruption is not merely the result of opportunism that arises in a vacuum, but exists within a structured ecosystem of actors, incentives, and processes. Across jurisdictions and fields, and considering both collusion and bribery, actors such as procurement insiders, rogue bidders, political elites, and intermediaries (like external auditors or consultants) interact with other peripheral facilitators like tenuously-connected shell firms or family proxies, within a textured institutional environment that often tolerates or tacitly legitimizes these transactional realities (Hudon & Garzón, 2016; Fazekas, Sberna, & Vannucci, 2021). These actors enact corruption through a range of instruments, from bid rigging to cost inflation to procedural sabotaging to evading regulatory safeguards, matched to particular features of institutional weakness. The modularity of this manipulation allows for networks to dynamically procure adaptation in response to reform pressure and scrutiny or following changes in political leadership, which affirm but do not necessarily exacerbate, the resilience of procurement capture.

However, in spite of this expanding canon of research focusing on actors and networks, there still exist a number of unresolved gaps that challenge the ability of this field to produce prescriptive, context-sensitive knowledge. One area that has garnered limited examination is the role of technological and institutional intermediaries, notably IT vendors, auditors, and union gatekeepers. While there have been nascent studies (e.g., Adjorlolo et al., 2025; Avdasheva et al., 2025) that begin to consider the means by which insiders or contractors can engage in corrupt behaviour using a digital procurement procurement system, to date, there has yet to be a systematic inquiry into the co-production of corruption via technical means. As blockchain and algorithmic platforms are increasingly embedded in procurement systems, it is vital to understand how the actors associated

with the digital design, implementation, and circumvention of digital safeguards lead to corruption. Without such inquiry, anti-corruption technologies will be performative, not transformative.

Additionally, while there have been adequate representations of institutional structures and macro power dynamics in the literature, the micro-level cognitive and organizational attributes of corruption are just being adequately studied through a scholarly lens. Research examining rationalization, moral disengagement, and peer reporting behaviors (Rustiarini et al., 2019b; Misran, 2024), suggest that the procurement actors operate in normalized deviance, or in environments where unethical behavior is rationalized for the sake of administrative efficiency or political loyalty to a respective office. Once again, these findings remain analytically disparate and rarely linked to the structural conditions that allow for this cognitional behavior. An integrated research program composed of organizational psychology, social network theory, and political economy would provide a more rounded picture of how individual dispositions interact with institutional logics to facilitate corruption and maladaptive behavior over time.

Another shortcoming in the existing literature is the empirical lack of challenging assessments on the behavioral response from corrupt actors resulting from the introduction of digital reforms. While digitalization is continuously lauded for increasing transparency, studies such as Bauhr et al. (2020) and Falcón-Cortés et al. (2021) demonstrate that technological or digital based reforms are often merely tactical displacements and not structural shifts. Corrupt actors - especially those with access to technical expertise or political cover - can often simply adjust their methods of engagement to new digital formality, in response to the reforms. In these studies of adaptive networks, Waxenecker and Prell (2024) and Lyra et al. (2021) demonstrate that a longitudinal approach represents the best opportunity to observe how procurement ecosystems change, or do not change, over time pre/during/post digital reform. In the absence of temporally relevant data, opportunities to make informed decision-making risk being impulsive and/or out of step with the real world.

These unresolved questions directly inform the theory and empirical orientation of this dissertation. While the literature highlights how actors - particularly intermediaries and digital actors - can reconstruct corruption networks, it has nuanced implications for how we think about institutional capture and policy resistance. It also expands corruption studies literature by explicitly examining anti-corruption technologies such as blockchain in relation to political and administrative systems that influence their use and productivity. Through a comparative, jurisdiction-specific analysis, this research will assess the intersection between blockchain, the law, regulatory instruments, and the technological landscape to find ways of mitigating procurement risks that exist in specific forms in Italy, Canada, and the United States.

The literature is unambiguous in one regard: to propel corruption studies forward, researchers must move beyond demarcated typologies and toward multi-scalar, interdisciplinary designs that identify the relationships between actors, institutions, and technologies. The study of procurement corruption is tactical, relational, and institutional. It demands tools—and tools of reform—that are

equally multi-dimensional. In this instance, rather than advocating blockchain as a silver bullet, we want to project it as a point where our empirical and theoretical assessments will converge on the interaction of law, governance, and technology. The challenge is to assess it with clarity and caution at different comparative levels.

Overall, the literature on corruption actors and procurement capture does not only provide a strong analytical base, but it also offers a powerful rationale for the comparative, mechanism-focused and contextual approach taken in this dissertation. The multi-actor configurations described - insiders, collusive bidders, intermediaries, political elites, and marginal facilitators - emphasize that corruption in public procurement is not just about bad actors; it is a systematic phenomenon based on institutional design, actor's incentives and policy regimes. While the literature has developed much richer typologies and political economy explanations, it has mainly been disconnected from the technological solutions that are proposed to combat procurement corruption, particularly blockchain.

This disconnect provides the first research gap addressed by this dissertation. That is, there is no integration of actor-based corruption modeling, as detailed above, and blockchain functional architecture. As discussed above, procurement corruption occurs through discrete observable mechanisms (e.g., bid rigging, cost inflation, or audit evasions), however existing blockchain literature tends to portray corruption abstractly, and does not systematically connect blockchain functionalities to risks associated with specific actor behavior or vulnerability in an institution. This research will address that gap by providing a mechanism-risk fit model, identifying corruption typology changes that may allow for blockchain-based solutions (e.g., smart contracts, timestamps, audit trails, or decentralized verification).

The second important contribution has to do with comparative institutional studies. Many studies look at corruption in a single jurisdiction, but fewer studies explore how legal traditions (for example: civil law, as in Italy, versus common law, as in Canada and the U.S.), federalism, or trajectories of regulated innovation may determine the capability for blockchain to be formally adopted and whether it maintains integrity in public procurement. While one of the goals of this study is to situate procurement corruption research between the monolithic constraints of procurement definition and the human dimensions of procurement, by comparing three different legal and governance regimes, this dissertation advances procurement corruption by considering how blockchain is facilitated across relative degrees of legal rigidity, administrative flexibility, and digital readiness, which is notably underexamined or omitted within procurement corruption research.

Furthermore, while previous studies (e.g., Bauhr et al., 2020; Fazekas et al., 2021) identified regulatory loopholes or poor regulation as facilitators or enablers, few studies have focused on investigating how regulatory experimentation such as sandbox regulations or procurement technology pilots can help or hinder the blockchain adoptions. This is directly tied to the third research question and fifth hypothesis of this study; that regulation is not simply a restriction on

blockchain innovation but can be a driver of the phenomenon depending on how it is institutionally framed and politically supported.

The final contribution is recognizing actor- and institutional-level resistance that is referred to in the literature, but not emphasized in the literature. The corrupt actor's typology presented in this chapter, particularly intermediaries, politically connected providers, and institutional gatekeepers, helps understand why even technologically viable blockchain unwillingly and occasionally necessarily collides with barriers to implementation. The current dissertation seeks to extend previous deterministic narratives of blockchain effectiveness to consider an integrated framework utilizing insights from institutional theory, political economy, and administrative behavior to examine why, where, and how blockchain might be resisted, co-opted, or stalled within the real-world context of procurement.

Finally, the literature points to another methodological gap that the Dissertation seeks to fill: the lack of models for adaptive, cross-jurisdictional learning when it comes to blockchain-based approaches to tackling corruption. There are broad similarities in how actors behave and how the mechanisms of corruption operate across countries, but the enabling legal, regulatory, and political conditions are entirely different. This research provides a way forward by presenting a contextual policy transfer framework which can enable blockchain governance models to be designed and/or adapted in a way that is scalable, while also being flexible to account for local legal traditions, institutional culture, and power structures.

To summarize, this chapter not only maps the terrain of corruption in the area of public procurement, but also accounts for the comparative, interdisciplinary and mechanism-specific approach this dissertation takes within the existing literature. It illustrates that while great strides have been made to understand the various ways in which corruption can manifest, there is still an urgent empirical need to investigate how, if properly connected to institutional conditions and actor propensities, blockchain can be a disruptor of ingrained systems of corruption. The dissertation takes a position within that juncture, improving our theoretical and applied understanding of anti-corruption innovation in public procurement contexts.

Synthesis and Implications: Procurement capture persists because it is organized in ways that credibly create complementary roles: insiders create windows of discretion; collusive contractors take advantage of discretion; political elites provide cover for the scheme and seal of legitimacy; intermediaries hard-wire the discretion into software and procedures; and marginal actors help conceal and spread the risk of capture. In recent years, research shows that these features can be monitored with mechanism-specific indicators (e.g., co-bid clustering, single-bid shares, timestamps anomalies, change-order ratios, and PEP-linked award) and formal scrutiny of compliance can still mask exception-by-rule (Sharma et al., 2019; Dávid-Barrett & Fazekas, 2019, 2020). As response, Table 2.1.1 pairs each of the risk to a specific DLT control as well as an auditable artifact (e.g., commit–reveal with a timestamped opening transcript; immutable change

order ledger; and public hash anchoring notices) within the table, it also annotates across an extensive range the legal predicates for admissibility and override by either the state or contractor (e.g., electronic-records statute and authenticity; due-process practices for reversibility; statutory channels for publication; and GDPR-minimized data transparency). In this, it bends the actor typology into a mechanism-to-Control fit developed in 2.2–2.2.2 and sets out an even more transparent basis for the comparative design introduced in the next of chapters.

2.2 Blockchain as an Institutional Infrastructure: Technical Foundations and Public Sector Applications

The modern conversation around state integrity and digital reform increasingly views Distributed Ledger Technology (DLT)—most commonly associated with blockchain—as an essential institutional infrastructure. In addition to its origin in cryptocurrency, DLT has introduced a new model of safe, trustworthy, visible, and verifiable data transactions, which lead toward greater legitimacy in public administration and "smart industries" (Bokolo Anthony Jr, 2023). This radical shift from the existing centralized database model to the distributed architecture requires different data processes and infrastructure that can help address ongoing concerns in public sector governance, especially around corruption and non-transparency that is difficult to get rid of through existing anti-corruption strategies (Transparency International, 2024). Public procurement presents a unique case with large flows of funds, which typically involve processes that are sometimes opaque. It will take new ways of thinking about public procurement to really address fundamental failures around corruption and non-transparency rather than merely relying upon legal formalism (Siino, Iezzi & Gara, 2024).

DLT provides a decentralized, distributed database that relies on an ever-growing, linked list of records that are cryptographically assured (Antal et al., 2021; Mutungi, 2023; Savadatti et al., 2025). The technical architecture of DLT has a number of properties that provide ways to lower the risk of vulnerabilities present in centralized systems. The first of these is immutability, the idea that once a record has been added to the ledger it cannot be changed or deleted. As Gietzmann and Grossetti (2021) explain, each new block in a blockchain includes a cryptographic hash of the previous block, creating a sequential chain that cannot be altered. Immutability is one of the most important properties of DLT when it comes to providing trustworthy audit trails for financial reporting compliance and reducing the risk for fraud and manipulation in central state systems (Mutungi, 2023; Savadatti et al., 2025). The cryptographic hashing functions (for example, Bitcoin uses SHA-256), create a digital fingerprint of the data that cannot be computationally reversed, or altered, without detection, thus providing strong assurance of the integrity of the data and its authorship (Gietzmann & Grossetti, 2021). Transparency, as a second property of DLT, allows authorized parties to view the contents of the ledger and is expected to provide accountability and lessen the information asymmetries that allow for corrupt practices in traditional opaque systems (Antal et al., 2021; Bokolo Anthony Jr, 2023).

Distributed ledger technology (DLT) networks are fundamentally disruptive of traditional governance models by distributing copies of the ledger across multiple nodes in a peer-to-peer network (Antal et al., 2021; Gietzmann & Grossetti, 2021) and, as such, this removes a single point of failure and dependence on a trusted intermediary, reduces the risk of error due to human discretion, and reduces the likelihood of collusion (Mutungi, 2023; Savadatti et al., 2025). A consensus mechanism maintains the integrity of the ledger to ensure that all nodes in a DLT agree on the validity and order of events before the addition of new blocks to the chain. This collective validation of transactions adds security to the system, and the system is less likely to succumb to the actions of individuals. Common validation mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). As such, PoW can be energy intensive, and thus less favorable for energy consumption, and PoS consumes less energy while maintaining security. PBFT is also a common mechanism used by permissioned DLTs as it allows for a faster and pre-agreed consensus on order (Khan, 202X). Ultimately, the choice of validation mechanism determines the role of trust delegation in a state system, e.g., use of PBFT can allow for a space of faster agreed consensus between a pre-agreed, and trusted, governmental or institutional node leading to benefits in auditing and accountability. Weingärtner et al. (2021), in demonstrating an example in public procurement, shows how blockchain allows for procedural integrity through pre-programmed consensus rules describing how system network designs, in this case permissioned designs should provide auditability while at the same time guaranteeing the approval of controlled input into the network while not sacrificing administration or regulatory demands.

Building upon these foundational properties, smart contracts represent a prominent application of DLT with significant implications for public procurement. Smart contracts, which engage in execution contingently to coded criteria on the distributed ledger, automatically execute agreements associated with terms and conditions when a predetermined event is indicated, eliminating the need for third-party intermediaries or processes (Mutungi, 2023). The notion of "code is law" (Lessig, 1999) has strong meaning in this context, as legal concepts in existing law and contractual agreements can be coded and executed directly through the software, which theoretically prevents any deviation from predetermined agreements. Smart contracts also enable execution without trust, meaning that contracting parties are not required to trust third parties, while also providing a robust language that cannot be easily interpreted by humans (Gietzmann & Grossetti, 2021). The case for smart contracts is concrete and pragmatic when automation circumvents discretion and accelerates the pace of compliance. Xu et al. (2021) note that smart contracts are being used to govern all areas from bid evaluations, supplier eligibility, payments for milestones, to delivery verification in pilot procurement systems in countries around the world, attesting to their practical application. That said, Xu et al. (2021) also highlight the importance of infusing real-time monitoring along with institutional mechanisms for fallback to deal with anomalies or deviations from the contracts. For example, a smart contract could automatically release payment to a supplier after the delivery has been verified by the action of delivery, while eliminating delays and opportunities for the supplier to solicit kickbacks (Mutungi, 2023).

Despite their classifying risks based on technology potential for automation and transparency, the incidence of enforceable legal sanctions associated with smart contracts in the procurement space is a continuing concern, especially when viewed from a civil law perspective. Sava and Dragoș (2022) explored possible compatibilities between smart contracts and EU procurement instruments and conveyed that the legal doctrine accept written contracts and procedural agreements while expressing interpretability and discretionary review as those are important factors that admittance of their use is threat of contradicting or undermining principles of proportionality, error correction, and administrative flexibility, - meaning it is something that can happen but there is no legal leverage in it to make it happen, so to speak. One might maintain that the with Blockchain-based procurements to begin gaining legal admission a necessity for adaptation of institutional practice needs to exist that incorporates a legal admission mechanism or disposition rather than adapted mechanism of recognition that distinguishes -ize codes, if then recognize form or act, meaning promoting a well form decision transition, and base acts in law. In this sense, it should be noted that smart contracts are only as reliable as the code that underpins it or injects that "interoperability" or "credibility". Chu et al., (2023), recognized vulnerability outcomes is it pertains to smart contracts as it applies to procurements, primarily, including, but not limited spent for reentrancy attacks, integer overflow and logic errors subsequently when use and application are assigned to public sector deployments and efficiency errors whatsoever may bring about contributory performance or even compulsive procurements and budgetary constraints or misappropriations. Normatively contemporary government agencies must acknowledge procurements contract code and be cautious of the leverage position that it affords them, and minimize or manage the risks associated with limitations or demonstrate incorrect applications as impartial to a public sector agency instead of regarding contract code as commonplace or resource for which should provide for administrative neutrality. Determining the nature of the contract code, correct applications of programming, and outcomes limits to indulged verification tools, contain static code analyzers, and participating in post intelligent monitoring or system auditing.

The relevance of different types of blockchains to public sector applications, particularly in procurement, is a critical consideration, as DLT encompasses a broader range of implementations than just the original Bitcoin-style blockchain (Gietzmann & Grossetti, 2021; Khan, 202X). Public, permissionless ledgers, such as Bitcoin and Ethereum, are open to anyone to read, write, and participate in consensus, offering maximum transparency and censorship resistance. They are characterized by a lack of central administrator and open access, allowing any user to join or leave the network at will (Gietzmann & Grossetti, 2021). However, their inherent properties often present challenges related to scalability (e.g., Bitcoin handling ~7 transactions per second, Ethereum ~15-20 TPS), privacy (due to open transaction history), and high energy consumption (especially with PoW) for large-scale governmental operations (Antal et al., 2021; Savadatti et al., 2025).

In contrast, private or consortium (federated) ledgers limit participation to an identifiable group of pre-approved organizations, hence offering more stringent control over access to shared data,

higher throughput of transactions, and increased privacy (Antal et al., 2021; Gietzmann & Grossetti, 2021; Khan, 202X). Examples of private ledgers include Hyperledger Fabric, which is a permissioned blockchain framework aimed at enterprise-grade applications, and R3 Corda, which has been developed as a consortium for banking (Gietzmann & Grossetti, 2021; Khan, 202X). The performance and privacy features implemented in these permissioned systems lend them to use in sensitive public sector applications like procurement, as they provide a controlled environment that balances transparency and confidentiality - highly pertinent to the management of sensitive public contracts. However, the trade-off is that they are not decentralized and could create entirely new tiers of centralization or system 'lock-in' if implemented poorly. If centralization does occur, it will create overlapping vulnerabilities to corruption through governance capture. Therefore, the decision of what typology to adopt in future DLT applications requires a complex balancing of competing values of transparency, control, efficiency, and security becoming even more pertinent in the discussion of the practical use of these technologies in Public Administration.

Apart from its transformative potential, the adoption of blockchain technology as institutional infrastructure entails major challenges and risks that leave room for questioning. Critics suggest that technology hype surrounding blockchain may often exceed those advantages in procurement contexts, and result in greater economic inefficiencies than more generic and simpler digital technologies, given the associated transition costs (Gietzmann and Grossetti, 2021). Some researchers assert that distributed ledger technology (DLT) is fundamentally unsuitable for legal regimes where a high degree of procedural discretion exists with respect to implementing normative rules or practices, due to the inflexibility of code, which hampers norms that require an administration to make decisions, or to assess or exercise judgment in particular contexts. Another relevant critique involves the potential for governance capture in private or consortium ledgers, where a reduced number of participants to the network can capture substantial control over the network and alter the decentralization mechanisms that are supposed to provide integrity. This potential is particularly acute in the public sector where private or economic elites capture control over the governance of the network. Indeed, the principle of immutability built into blockchain can be fully at odds with many foundational principles evident in data privacy statutes, such as the General Data Protection Regulation (GDPR), and especially Article 17 (Right to Erasure) providing additional difficulty for public sector data managers if they consider deploying blockchain technologies. This complexity, if we adopt a legal analysis as our starting point, leads to legal and technical challenges that must be addressed with innovative solutions including hybrid models that utilize both on chain, off-chain storage, or proof of zero-knowledge (Savadatti et al., 2025). Furthermore, concerns exist about the massive amount of energy consumed for certain consensus mechanisms, especially Proof of Work consensus mechanisms, thus creating environmental and economic challenges related to the widespread adoption of blockchain technologies within the public sector, and other big questions related to the sustainability of blockchain technology reform. These risks reveal that establishing blockchain technology as an effective secure, institutional infrastructure, even with robust technological solutions, requires a

better understanding of the limitations, unchecked outcomes, behaviors, and establishing accountability within the governance process that extends beyond the technological layer.

The successful implementation of blockchain in public procurement depends not only on its technical design, but also on integration within institutional structures, policies, and norms. The spread of reforms occurs when technologies are considered legitimate and consistent with existing practices and norms, through cognitive, mimetic, and normative pressures to adopt (Suchman, 1995; DiMaggio & Powell, 1983; Fountain, 2001). Consistent with this, Troisi (2022) illustrates how institutional pressures and organizational norms can influence behaviors and compliance in environments prone to corruption, and in a similar vein, institutional pressures will influence whether procurement bureaucracies accept, reject, or simply symbolize compliance with technologies that enhance transparency, such as blockchain. Policy structures also reflect this logic: for example, the EU blockchain strategy characterizes decentralized ledger technology (DLT) as a cross-border infrastructure for public service subject to regulatory compatibility, and the UNCITRAL Model Law and Model Guide puts transparency, efficiency, and fair competition—which DLT has the potential to address—at the forefront in neutral settings when you add in legitimate publication, evidenced by records, and redaction standards (European Commission, 2020; UNCITRAL, 2011, 2012). Practically, there are also examples of gradualism through capacity: pilots like Colombia's the SECOP emphasize proof of interoperability with state-led e-procurement, and South Korea staged its planned deployment to emphasize the governance design most able to support bureaucratic systems (MSIT, 2020; World Bank, 2021). Thus, blockchain effects will not simply be dictated by its technical architecture, but by its institutional legitimacy, capacity, and governance.

In summary, as a form of DLT, blockchain technology provides an attractive opportunity for improving integrity and efficiency in public procurement through its attributes of decentralization, transparency, immutability, and smart contracts. However, successful implementation as an institutional infrastructure will require overcoming serious technical barriers relating to privacy and scalability, as well as important legal and regulatory considerations, and socio-political influences and resistance from actors within organizations. The choice of blockchain typology, consensus mechanisms, process for ensuring enforceability of the law, and governance of data, should not be treated purely as technical considerations, but as critical policy considerations that will determine whether this technology might actually disrupt entrenched corrupt equilibria, as opposed to simply displacing them in settings that may be used nationally. These reflections on the relationship between the possibility of technology, and the realities of the institution, form an important link in understanding the role of blockchain in the reform of public sectors, and serve as a foundation for comparing the approaches to legal and regulatory and implementation challenges in Italy, Canada, and the United States.

In order to implement the actor typology, this study engages in pre-specification of a mechanism—risk fit for each lifecycle window, definable observable indicators functional in the procurement data/text, and the precise DLT controls that could overlap the relevant behaviors that are legally

required as per the legal requirements. The pre-specification would block ex-post rationalization and promote comparability across jurisdictions (Italy/EU, Canada, U.S.).

Public (permissionless) ledgers maximize transparency and independent verification, but they impose constraints that are relevant for procurement workflows: throughput is deterministic but lower, latency can vary with scale, and full-ledger transparency creates issues with confidentiality of pre-award materials. Their major benefit for the public sector is independent verifiability of integrity: storing notices, bid-opening transcripts, or payment hashes on a widely observed chain strengthens the integrity of a record against collusion at the time of occurrence and retroactive changes. Permissioned ledgers, on the other hand, offer predictable throughput and latency, native access control to protect bid confidentiality and role separation, and explicit validator control by, for example, contracting authorities, audit offices, or courts that meet statutory accountability requirements. The trade-off is that integrity is evaluated based on the rigor of consortium governance and change management to resist capture (2.2.2 and 2.4, and Table 2.1.1).

The hybrid approach accounts for these tensions for procurement by using a permissioned ledger as the system of record for tender, evaluation, contract, and payment events, while enforcing confidentiality, role-based controls, and retention. Hybrid approaches enhance evidence and assurance by periodically anchoring critical states of the process to a public chain so as to gain independent timestamping and tamper-evidence. In practice, this means that sealed-bid commit–reveal and evaluation logs can remain within an access-controlled domain, while statutory publication can continue, the high-assurance proofs (hashes, receipts, signatures) can be exported for audit and litigation processes. Governance safeguards - independent oversight nodes, change-control charters, exit and portability testing, evidence-packaging protocols, will mediate consortium risk to support both admissibility and reversibility requirements (which are further discussed in 2.2.2 and 2.4). This bridge motivates the typology choices that are made across lifecycle in Table 2.1.1 and provides the foundation for comparative design developed in the following chapters.

2.2.1 Blockchain Typologies and Trade-offs for Public Procurement

Public procurement processes are increasingly experimenting with blockchain to reduce the risks of corruption, though typology type—public/permissionless, permissioned/consortium, or hybrid—frames the design space for transparency, privacy, and legal compliance. Typologies are not neutral; they broker power, set audit affordances, and limit stakeholder participation based on institutional and regulatory contexts (Sedlmeir et al., 2022; Kassen, 2021)

The identifying and most basic difference in blockchain architectures is between public/permissionless blockchains (e.g., Bitcoin, Ethereum) and private/permissioned blockchains (e.g., Hyperledger Fabric, Quorum). Public blockchains enable any participant to access or validate the blockchain which leads to the greatest transparency and strongest resistance to censorship within a given network. Yet, public blockchains are often hampered by scalability, slower consensus methods, and the need to expose details that could compromise privacy—all of which

compromise their utility for certain types of procurement (Monrat et al., 2019; Sedlmeir et al., 2022; Sung & Park, 2021). In contrast, permissioned or consortium blockchains only allow validation by a small set of authorized nodes, which helps provide greater control, privacy, and transaction accessibility. With these advantages comes a cost of reduced decentralization, the ability for validators to collude with each other, and technical lock-in that could inhibit interoperability and flexibility for governance in the future (Diadia et al., 2023; Baranwal, 2020; Siddiqui et al., 2023).

The existing literature indicates a burgeoning interest in hybrid or enterprise-consumed blockchain architecture in public procurement, especially in jurisdictions where accountability and auditor-ability must be weighed against privacy and efficiency (Ibrahimy et al, 2022; Nodehi et al, 2022). For instance, deployments on Hyperledger Fabric enable governments to limit visibility of procurement's records to designated stakeholders while retaining tamper-evident trust through Merkle tree verification (Diadia et al, 2022). These systems have also raised concern with the opaque governance of validators and institutional excessiveness, notably in circumstances where political partisanship or disaccountability are factors in a validating consortium (Carvalho, 2019; Kassen, 2022; Bai et al, 2022). Such processes are not explicit technological challenges, but reflections of the political economic dimension of procurement governance, where decentralization could inhibit or constrain agency to preserve control.

Moreover, while the energy consumption debate is most often considered in those discussions surrounding public blockchains, it is also considered in terms of procurement-related solutions, too. Given their environmental impact and inefficiency, high-energy consensus mechanisms, such as Proof-of-Work (PoW), are generally deemed unsuitable for use in most public sector contexts (khalfan et al., 2022; Sedlmeir et al., 2022). That said, many systems implement low-energy alternatives (such as Practical Byzantine Fault Tolerance (PBFT) and Proof-of-Authority (PoA)) particularly within networks that are permissioned (Diadia et al., 2023; Siddiqui et al., 2023). While they are low-energy and efficient, many of these consensus mechanisms hold centralized validation power, raising critical questions about their long-term resilience and accountability. In general, the definition of blockchain type is not strictly a technical decision, it is also indicative of a broader spectrum of trade-offs that exist between efficiency, control, and integrity.

A primary governance risk in permissioned or consortium blockchains used to support public procurement is collusion among validators and possible institutional capture. Unlike the decentralized consensus of public blockchains, where transaction validation occurs among a largely anonymous pool, permissioned blockchains confer validation status to a limited number of entities—frequently comprised of government agencies, IT contractors, or other selected institutions. This structure results in the risk of cartelization of the validator pool, allowing the validators to coordinate on the manipulation of what procurement data is validated, ordered visibility of records, or altered records in the past with plausible technical justifications (Carvalho, 2019; Bai et al., 2022; Sedlmeir et al., 2022). These are not unknown risks; implementations in Latin America and Eastern Europe documented how technical consortia, which in theory provided

operational control, increased discretionary power in the name of digital reform (Bolívar & Prados, 2022; Roeck et al., 2020).

The concept of a "decentralization illusion"—where the appearance of technical robustness conceals a tightly controlled validator structure—has been substantively discussed in the literature. Bolívar and Prados (2022) note that in instances where the smart contract code, the list of validators, or an audit log is not made publicly accessible, any ostensive transparency of blockchain is merely a performance. Sánchez (2019) critiques early use cases in the European context and shows how many of the "decentralized" procurement pilots used to develop the paradigm could not be distinguished from conventional e-procurement systems, given the presence of opaque access controls and centralized administrative keys. These insights are particularly relevant to anti-corruption approaches in public procurement, where openness and verifiability are not merely technical components, but institutional features that seek to protect against rent-seeking and discretion-based favoritism.

In contrast, public blockchains, such as Ethereum, provide an extreme level of transparency through a fully replicated ledger and open smart contract deployment, allowing for public auditability of procurement flows, immutable record-keeping, and resistance to unilateral manipulation (Monrat et al., 2019; Mezquita, 2020; Sung & Park, 2021). As an example, if a procurement contract were deployed on Ethereum, it would be possible to include conditions of execution to execute the contract which would be verifiable by citizens, watchdogs, and oversight institutions. This transparency comes with trade-offs in scalability and confidentiality. Baranwal (2020) states that core public chains are unable to process the vast array of procurement data involved in large-scale procurements without compromising throughput and/or incurring a prohibitive expense in terms of data storage capacity. Additionally, if state secrets or sensitive procurement data (e.g. identities of bidders, contract values, etc.) were to be excessively disclosed without using privacy preserving (e.g. zero knowledge proofs or off-chain aggregation layers) technologies, government officials may be unintentionally exposing themselves to secondary risks (e.g. lobbying strategies, manipulation of bids, etc.).

These opposing logics highlight the governance asymmetries underlying blockchain types. In permissioned chains, institutional control and system efficiency are privileged, at the expense of decentralization and visibility; in contrast, public blockchains favor openness, the most public commitment to decentralization, accepting the loss of operational control, to achieve maximal visibility and immutability. In contexts with low institutional trust, histories of elite capture, showing procurement data on a global ledger that will be visible to everyone could simultaneously deter elite manipulation, as well as empower civil society (Sánchez, 2019; Andrade et al., 2024). Meanwhile, deploying this use-case in higher risk or otherwise sensitive environments, the public nature of a public chain could bring with it the potential for institutional resistance to blockchain due to perceived issues around sovereignty, privacy, or political risks.

The studies conducted by Diadia, Tamgno, and Kora (2022, 2023) on the use of Hyperledger Fabric utilized in public procurement systems is one of the key examples of the operational advantages and governance limitations related to permissioned blockchains. The authors describe a blockchain enabled dematerialized procurement system that utilized Hyperledger Fabric with an Open Contracting Data Standard (OCDS) integration, where the procurement system envisioned to provide a transactional immutable ledger that would account for all decision points relative to procurement, from the issuing of the tender to assigning the contact, while enhancing integrity, transparency and traceability. The authors provide examples of how permissioned systems allow for reductions in the opacity of processes and tampering while at the same time promoting interoperability with existing data standards.

However, as the authors point out, the above advantages rely entirely on how validator access and smart contract governance are structured. In particular, reliance on a trusted source of validators (primarily government or contractor representatives) raises potential concerns of validator collusion, particularly in constrained environments of low external oversight. The risks are increased given that there are no public anchoring mechanisms in place - such as hash commitments to external blockchains - that would allow civil society or independent auditors to verify data accuracy without access to the distributed network (Diadia et al, 2023; Siddiqui et al., 2023). This illustrates a similar trend across the literature; while permissioned chains might leverage compliance and automate processes, if governance is not independently verifiable, the end product mimics the gate-keeping logic of legacy procurement platforms.

Additional similar findings can be seen in Nodehi et al. (2022) who develop the Enterprise Blockchain Design Framework (EBDF) and apply the framework to current e-procurement use cases. The EBDF evaluates different system configurations across four dimensions: privacy, auditability, scalability, and trust among stakeholders. According to Nodehi et al. (2022) in pre-established e-procurement use cases, a permissioned framework is preferable when confidentiality and control of an internal process is valued more highly than the ability to view the process publicly. For instance, when provisions are made in very sensitive sectors such as defense, healthcare, or large infrastructure projects, consortium-based blockchains can support selective disclosure of the terms of the contract while supporting cryptographic evidence of the underlying data integrity. However, permissioned arrangements also present design challenges: the more the system demonstrates centralized control (to achieve confidentiality objectives), the greater the likelihood that the system is not insulated from institutional capture or ranch manipulation.

This tension is also visible in examples from sectoral cases, such as Kim and Kim (2024) who analyse blockchain use in procurement of construction projects. Using a permissioned implementation, the authors note improvements in real-time reporting, verification of payments, and compliance with payment triggers/contract milestones. They note that the governance structures set up for blockchain systems lack multi-stake relationships; current decision-making structures are determined by contracting agencies or information technology vendors and often fail to represent the voices of others that are stakeholders/whom may be affected. The findings of Kim

and Kim (2024) closely align with the critique of governance; that is, the tendency for permissioned networks and elite consortium models, amongst others, to entrench traditional institutional hierarchies/relationships, unless system design anticipates the decentralization and redistribution of verification authority and thus is capable of securing accountability across actors (Carvalho, 2019; Bai et al. 2022).

In conclusion, the use of permissioned blockchain systems like Hyperledger Fabric for procurement represents an example of the possible operationalization of structure, allowing for a workflow automation, data integrity, and the compliance with relevant policies. The trade-offs concerning transparency, validator independence, and public oversight, however, remain unrealistic. Critical engagement with the trade-offs is necessary in relation to anti-corruption and accountability: if a blockchain system supports organizational opacity—no matter how sophisticated from a technical perspective—is merely a digital form of organizational accountability. A blockchain like Hyperledger Fabric may not represent the operationalization of a new mode of governance.

Unlike permissioned blockchains that have regulated architecture, permissionless blockchains, such as Ethereum or Bitcoin, represent a radical shift in governance: public validation, distributed governance, and immutable transparency. These attributes make blockchains particularly attractive as tools in an anti-corruption public procurement reform context, particularly in contexts where public trust in institutions is weak or where traditional oversight is not working. Mezquita (2020) and Sánchez (2019) emphasize that with public verification of the transaction, which includes contract awards, bidders, and payment flows on a public ledger, there is a level of accountability that could not be replicated in permissioned environments.

A noticeable benefit of public blockchains is that they allow open-access smart contracts, which is code that automates contractual logic that is uploaded to the ledger in a permanent way. This provides the opportunity not just for institutional stakeholders to monitor procurement, but civil society organizations, journalists, or citizens to monitor the process in real time (Bolívar & Prados, 2022; Mezquita, 2020). For example, a tender process on Ethereum could potentially automatically reject late bids; enforce payment timelines; or initiate audits in the event of contracting delays. Such actions would, thus, allow for real-time and precise auditing of procurement due to the immutability of blockchain and the permanence of smart contracts. While traditional e-procurement methods utilizing permissioned chains or traditional tendering and contract management systems could implement auditable logic without the sub-transactional elements of real-time auditing or heightened trust; this type of logic is transparent and defers trust to various validators rather than one single validating party. According to Sung and Park (2021) in their analysis of public blockchain, this is a move away from business as usual. It flips public-auditable data for the social good from being an exclusively discretionary asset for public sector actors into a true common good by allocating open-access on the blockchain based on a pre-definable and verifiable logic.

The trade-offs between convenience and disclosure are notable. Public blockchains do not guarantee any form of privacy, such as the name of the contractor, the size of the bids, or even the specifications of the project; unless privacy-enabling technology is employed such as using some form of cryptographic protocol. Englehardt (2022) argues that the major challenge with public blockchains is that any information relevant to the procurement process would be visible to everyone on the public blockchain network unless cryptographic techniques are employed if applicable. Privacy-enabling technology such as zk-SNARKs or multi-party computation offer privacy and transparency, but have both high technology and performance overhead (Chen et al., 2022; Baranwal, 2020). Public sector procurement agencies face the challenge posed by a public blockchain: we want the system to feel transparent and accessible, but the risk is their procurement and contract would expose information that an actor would exploit to better a competitor in the marketplace or weaponize it for political purposes.

Scalability remains a challenge as well. Public chains implement consensus algorithms that demand computing resources (e.g., Proof-of-Work (PoW) or Proof-of-Stake (PoS)), which limits the transaction throughput and work-processes associated with high-volume procurement operations (Monrat et al., 2019; Sedlmeir et al., 2022). The storage costs and execution costs of using a public blockchain are significant, which is a barrier to implementation for many governments in the Global South that do not have any digital infrastructure in place. These chains have also been implemented selectively or phased out as hybrid implementations, which makes a claim about decentralization moot. A typical case is the on-chain storage of selected procurement metadata and off-chain storage of the full data into a central repository (Siddiqui et al., 2023; Andrade et al., 2024).

Governance also figures as a challenge. Despite the perceived decentralization that public chains promote, they can also have instances of informal centralization, ranging from the role of mining pools to the role of protocol developers and core node operators. Sánchez (2019) warns that without institutional adaptation; public chains can be taken over by technical experts that manage up a smart contract standard in a way that influences system upgrades and decision-making processes after the fact. Further, instruments of public procurement tend to exist in legal systems where redaction, minimization, and judicial review of information are mandated, which electronic stewardship protocols do not easily accommodate.

As we enter the realm of the adoption of ‘public’ blockchain for procurement, it becomes essential to consider the balance of benefits and trade-offs. Public ledgers are great for integrity of the data and verifiability from citizens. But it will never be able to address workflows that include sensitive tenders, national-security considerations, or strict data-protection obligations. Hence, existing literature has centered around hybrid architectures that provide the benefits of public- chains to build trust and visibility, but suspend the privacy-sensitive logic to other technical environments (off-chain or permitted). The existence of hybrid models reinforces the point of distinctly matching ledger selection with governance, legal structures and scalability issues, rather than simplifying

the selection as merely being “public vs. permissioned” (Kim & Kim, 2024; Khalfan et al., 2022; Nodehi, Zutshi, Grilo, & Rizvanovic, 2022; Siddiqui, Tansen, & Abdalla, 2023).

Indeed, hybrid configurations commonly involve off-chain or private/consortium ledger storage of tender documents and transaction information while utilizing a public clearly-defined set of hashes evidencing tender artifacts, milestones, and amendment claims. In these models, the architectural separation creates beneficial disclosure capacity, enables role-based access, retains end-to-end verifiability, and limits personal or commercial sensitive data is exposed. The case is true for both enterprise design models for e-procurement ecosystems they propose and for everyone’s vicinity, as assessed procurement workflows emphasized governance clarity, standardization, and interoperability (Khalfan et al., 2022; Nodehi et al., 2022).

A review of Canadian and US public-sector efforts highlights additional trade-offs. In Canada, the National Research Council’s Industrial Research Assistance Program demonstrated a pilot around publishing grants and contributions via Ethereum, and a public IPFS Explorer ('Catena'). This pilot showed great verifiability of data on a public ledger, but also raised governance questions around the publishing project when there is a single agency publishing node (National Research Council Canada, 2018a, 2018b). In the US, the FDA's Drug Supply Chain Security Act (DSCSA) Pilot Project Program offered lessons synthesized from 2021 end-to-end traceability pilots where interoperability, data quality, and operational adoption, stood out as limitations. As the majority of the pilots were permissioned, it is not appropriate to generalize claims about energy consumption from the project (U.S. Food and Drug Administration, 2023). In Vienna the ‘OGD – Change Protocol and Notarization’ pilot used blockchain-based time-stamping and notarization, to evidence open-data records’ integrity and time-of-existence, which is a classic back-end-internal integrity use-case, as it allows proof without using full disclosure, but allows independent verification (City of Vienna, 2018).

Italy also provides a window into the lesson of state-backed traceability as opposed to procurement, but the lessons are the same. The Italian Ministry of Economic Development (MiSE) certified a feasibility study with IBM in 2019 to design a blockchain solution tracking ‘Made in Italy’ supply chain traceability (textiles). Their report surfaced the recurring impediments to an appropriate use of blockchain technology, including interoperability, governance, and standardization—similar to the impediments faced in procurement—support incremental and standards-aware adoption choices (Ministry of Economic Development & IBM, 2019).

In summary, the conversations in the literature and the public-sector pilots signal that utilizing hybrid blockchain architectures—publicly anchored, supplemented by permissioned/on-chain processing—proposes a realistic option for responding to desires for transparency and accountability to avoid corruption, as public sector agencies are still able to support legal requirements, privacy, and feasibility (Kim & Kim, 2024; Khalfan et al., 2022; Nodehi et al., 2022; Siddiqui et al., 2023).

Nodehi et al. (2022) provide a methodical approach to designing these hybrid systems with the EBDF (Enterprise Blockchain Design Framework). One of the aspects provided by the EBDF is the dimensions to consider - such as stakeholder governance, privacy needs, transaction frequency, and performance requirements - for choosing typology and network architecture. When applied to procurement contexts, the authors provide examples of modular designs based on the intended procurement stage: for example, bidder registration could occur on a private ledger with identity verification and contract execution events posted on the public chain. This can serve an anti-corruption objective as it minimizes much of the undesired discretionary ambiguity or opacity, while allowing the operators essential operating discretion.

Interoperable layering is front and center for these hybrid models. Public procurement processes often rely on a multitude of actors (ministries, regulatory organizations (government), - auditing organizations (government), bidders, and suppliers) who have differing statutory and organizational obligations. There is no single blockchain typology able to fulfill all these situations (Kassen, 2022; Khalfan et al., 2022). Therefore, interoperability standards like the Open Contracting Data Standard (OCDS) can be paired with blockchain systems, and other public formats, enable procurement activity data recorded in multiple design modular layers remain semantically compatible and readable. As the case studies by Diadia et al. (2022, 2023) illustrate, the ultimate success of their Hyperledger Fabric implementation, required to incorporate and muddle through the design of the smart contracts, connecting the labor to the structure of the OCDS schema, and interfacing with Auditor platforms, required a collective process.

While hybrid architectures lend a certain flexibility, they also create their own coordination and governance issues. According to Sung and Park (2021), interoperability between blockchain layers must have some sort of standardized identity management, consensus on data types, definition of communication protocols for secured cross-chain communication. Hybrid systems, without these elements, can result in fragmented silos in these systems. Additionally, hybrid designs can still encounter base dilemma constraints: a) which actors control the permissioned layer; b) how are smart contracts managed and updated; c) is there a legal framework for identifying enforceability of on-chain events in off-chain dispute adjudication the parties agree to?

The literature recognizes that a number of pilot programs are emerging with government funded blockchain initiatives, especially with projects in Latin American, South Asia, or parts of Europe, considered hybrid. Countries such as Brazil and Mexico regularly disclose the outcomes of procurement record implementation conceptually in from publicly available ledgers while relegating institutional internal decision-making into private chains or institutional records. (Bolívar & Prados, 2022; Andrade et al., 2024). This dual state aligns collaboration and reality for many users: Procurement transparency does not require radical layer-specific openness but a layer which enables key integrity aspects could be verified externally without requiring the operators lose internal operational integrity and/or the constraint of some legal conditions.

In conclusion, hybrid blockchain architecture serves as an situational variant of the public–permissioned spectrum. Hybrid blockchain architecture can also be viewed as a custom–modular tool-box that can attempt to reconcile the tensions of being open, efficient, and controllable. That said, hybrid blockchain architecture must take the form of governance, use interoperability, and external validation in order to avoid being re-branded digital bureaucracies that operate in opaque environments.

Evaluating blockchain typologies for public procurement requires both a qualitative analysis of distinct typologies and an assessment of multidimensional trade-offs of practical relevance in governance structures. The literature reflects the underlying importance of five key dimensions of significance from an analytical perspective: scalability, energy efficiency, privacy, data security, and governance. All dimensions intersect with each other and often only exacerbate tensions between technological design elements and institutional values, especially in relation anti-corruption practices and the integrity of procurement.

The first dimension, scalability, describes whether a blockchain system has the capacity to meet high volume transaction processing demands in respect to reasonable latencies. Scalability is an issue for both public, permissionless blockchain in practice and in principle. This has been noted before by both Monrat et al. (2019) and Sedlmeir et al. (2022) that public chains, such as Ethereum or Bitcoin, are constrained at the processing of transactions sequentially, plus relying on consensus globally distributed, hence when a chain is exposed to peak loads creating bottlenecks the real-word volumetric performance limitations can have devastating effects on a responsive and usable public procurement system. In comparison, permissioned blockchain such as Hyperledger Fabric or Quorum tackle these issues by partitioning transaction processing, using parallel endorsement, and using consensus protocols like PBFT that each allow for significantly more transaction throughput (Diadia et al., 2022; Siddiqi et al., 2023).

Related to scalability is the question of energy direction, particularly in the current climate-conscious governance environment. Essentially, public blockchains that work using Proof-of-Work mechanisms may be compellingly questionable in terms of the energy consumption required for consensus (Sedlmeir et al., 2022). Although Ethereum's shift to Proof-of-Stake reduced energy consumption, a even though low volume permissioned blockchain does function with constrained resources, it does benefit from less known minimal validators and deterministic consensus protocols (Khalfan et al., 2022). In this respect, a dimension of energy usage is more than technical–it can help or hinder political acceptability, justify cost, or reach sustainability targets desired in public procurement modernization strategies.

Privacy is another key dimension of difference. Public blockchains mean it is difficult (if not impossible) to have default privacy. By design, in public blockchains all transactions are visible to all participants as a condition of transacting on a blockchain. While these traits are valuable as part of anti-corruption, the absence of any expectations of privacy represents a substantial risk for sensitive procurement examples such as defense contracting, distinctive health services, or large

infrastructural commitments. As Baranwal (2020) and Chen et al. (2022) described, introducing privacy by way of zero-knowledge proof, commit–reveal, or referencing data off of the blockchain require not only computational power but minor complexity taper which generally results in an asymmetrical design that lacks the elegance and resourced trustless ideal that is offered elsewhere. Permissioned blockchains add privacy in the form of channel access, private transaction subnets, and pools of organization data partitions that were deemed important when selecting deployment contexts allow blockchain use (Diadia et al., 2023; Kim and Kim, 2024).

Regarding the component of security, the literature has indicated that there are strong systems of data integrity and tamper-resistance being offered by both typologies, albeit under different architectures. Public blockchains use mass decentralization and economic disincentive (through staking or mining rewards) to prevent attacks, while permissioned systems use organizational morality and whitelisting. Some of the concerns here is being more prone to (some might call it) internal corruption through collusion with the validators or misconfiguration of a smart contract with no tools for externally verifying the validity of the transactions (Carvalho, 2019; Bai et al., 2022). That said, while permissioned systems might minimize outside threats to transactional integrity, these systems are more likely to suffer from internal governance risk(s).

Lastly, governance structure delivery is arguably the most politically significant trade-off. Governance in public blockchains tends to feature open-source development. In this model, developers can propose and implement upgrades and changes to the protocol, which the developer community hashes out and discusses together. This decentralized governance increases the resilience of the system; however, depending on how an organization chooses to utilize the protocols, it may be more difficult for them to align systems, or comply with legal laws or policies. On the other hand, governance in permissioned formats is often centralized (or federated), through which governance meetings can amend, discontinue, or update agreements, integrate policies, and/or facilitate regulatory texting (Nodehi et al., 2022; Sung & Park, 2021). However, as Bolívar and Prados, (2022) and Sánchez, (2019) discuss, the centralized flexibility could be problematic, as this might referentially re-introduce opacity by allowing actors in the organization to operate without the transparent conditions that blockchain allows.

In bringing together these factors, one of the most idiosyncratic observations across the literature is that no architecture offers the optimal solution for all public procurement purposes; which is why the selection of an architecture ought to be determined by institutional risk mapping, legal obligations, and policy priorities. Trade-offs must be made, but the allocation of the trade-offs, or, who takes the hit, who controls the system and who is able to verify the results, is what determines if a blockchain procurement platform is contributing to anti-corruption, and promoting the public interest.

The implications of how these typologies are operationalized in the public procurement space are most visible when considering the real-world consultation, anti-corruption cases where the design of the system reflects institutional priorities and political economy constraints. Comparative case

studies (of Brazil, Italy, and Estonia) provide some examples of how governments approach different blockchain configurations dependent on their local governance settings, risks of corruption, and operational capacity.

For instance, Brazil's recent advancements in public contracting have favored more hybrid architectures - permissioned data management and public verification. Bolívar, and Prados, (2022) documented municipal procurement platforms in São Paulo and Rio de Janeiro's decisions to experiment with publishing procurement milestones and financial disbursements on an Ethereum sidechain, while still having the records of vendors identity and negotiation of contracts on private nodes controlled by the treasury and courts. The hybrid architecture allowed governments to publish public milestones, while having the flexibility and discretion to protect commercial insight within isolationist organizational structures, something that public statement practices have been ever-growing in demand for since their scandals of corruption (e.g., Operation Car Wash), while being legally mandated to not breach the data of a private firm's client confidentiality and or fiscal responsibility. The result is a typology that supports public validation for key events—such as contract award and delivery confirmation—while keeping more sensitive data within organizational departments.

In Italy, studies by Roeck et al. (2020) and by Diadia et al. (2023) also show a similar trend but only stronger towards institutions control and process formalizations. Indeed, the Italian public procurement agencies have been implementing several Hyperledger Fabric to record vendor registration, procurement planning, and payment flows. These implementations tried to automate compliance first and auditability in a controlled environment. Such attempts to favor compliance and act in a certain way with public institutions that have had a history of granting discretionary contracts, place the major risk of creating a system that will keep the same level of opaqueness as before, as Carvalho (2019) and Sánchez (2019) warn about. The case of Italy demonstrates that simply opening your code's technical decentralization to the public will not guarantee that there are "political" accountability mechanisms, it will only help if it offers independent scrutiny with open access to the validation precautions to those mechanisms.

Estonia showcases a poignant contrast. Widely seen as a champion in digital governance, Estonia's experimentation with blockchain for public procurement primarily used for data integrity, rather than relying on transactional transparency. In Estonian forms and processes, the systems invoked blockchain as a secure audit trail in accordance with the public procurement process with the framework securing the prevention of unauthorized alteration - it did not perceive value in making contract detail public. This typology suggests a high level of institutional trust to create a strong legal framework making use of the blockchain back end to provide the artifice of integrity and not as a medium for transparency. In contexts with a high level of institutional trust, this is likely a valid use case but is probably not sufficient for anti-corruption purposes in jurisdictions experiencing opacity and collusion as a result of the absence of any defining practices.

The typology examples presented here raise an important question regarding the scholarship: choosing which typology is not only a technical decision, it is also a governance choice, and is therefore revealing the institution's intent. Where governments adopt principles of public oversight and civic engagement prints the likelihood of utilizing public or hybrid chains (with public validation layers) as techniques to facilitate public access. By contrast, where governments use principles of internal controls, compliance, and risk mitigation, governments are more likely to use accepted systems, even if that acceptance limits external verification opportunities (Andrade et al., 2024; Nodehi et al., 2022). Therefore, typologies may serve as a constrained proxy for the level of political will to act on corruption, and typologies should be assessed for their conceptualization of that political will.

Further, typology determination also serves to mediate how systems present themselves to corruption. In low trust environments, public chains may be able to preserve immutable evidence trails which may disincentivize contract modification or retroactive fraud. In high trust, but low resourced contexts, permissioned chains are a way to reasonably automate compliance and (slowly) asset without having to reconfigure existing particular workflows. However, in each case typing may be mistaken by authors for a technical fix. The extant literature cautions that blockchain should not be accepted (or anticipated) as a technical fix without corresponding reforms: independent audit bodies, public procurement data access, and substantive standardization and institutional safeguards.

Beyond structural arrangements, the governance logic embedded in the design of smart contracts is critical to the effectiveness and impact of blockchain-based procurement systems. Simply put smart contacts define automated procurement rules - bidding windows, compliance protocols, or payment terms. Their design caters not purely functional logics but also normative choices about accountability discretion and enforcement. The nature of the underlying blockchain constrains and permits these design elements, establishing who can design, audit, and execute smart contracts, and the conditions for doing so.

On public blockchains, smart contracts will be open source and accessible to any participant in the network. This kind of architecture makes it is possible for participants to verify the designs and logic of smart contracts, which limits the potential for discretionary alteration of rules and eliminates the possibility of back doors, enabling them to check for logic of execution, or how it will determine the results. As Mezquita (2020) and Bolívar and Prados (2022) point out, these instances of architectural transparency are particularly valuable when integrating the procurement process with contracting for large capital works involving politically exposed persons. For example, a contractual bidding process, designed for Ethereum, could embed rules and logic to comply with timelines, set bid levels to reject bids less than actual costs, and provide live details on the evaluation process, without reliance on an internal bureaucracy. This kind of design is technology oriented rather than based on discretion and provides a control technology that is guaranteed by public code. They reduce the opportunity for fraud, favoritism, and procedural manipulation.

However, these aspects of design transparency for adopting blockchain applications assume a high level of technical literacy and institutional willingness to be open. In many environments, procurement authorities err on the side of caution when drafting contract codes that they are afraid to expose to the public due to concern of being litigated, concerns of publicity, or concern about their competitors taking advantage of their work by politicizing it (Sánchez, 2019; Sung & Park, 2021).In addition, many existing provincial- or regional-based law and legislation have not recognized legal authority or admissibility of carrying out smart contracts in the same way as commercial contracts if a dispute arises. This consideration has resulted in some governments referencing permissioned over public blockchains, where the design and verification methods for auditing will be managed the trusted administrator or the oversight body, balancing the use automation with dependence for legal and political discretion (Kim & Kim, 2024; Siddiqui et al., 2023).

Nevertheless, in permissioned environments, smart contracts frequently become an administrative tool with a minimal impact on governance innovation. While it may use procurement logic, it does not have any external auditability or public triggers, thus removing the deterring factor to carry out corrupt practices. According to Nodehi et al. (2022) and Khalfan et al. (2022), this removes the concept of trust lessness associated with the blockchain, enabling organizations to use smart contracts as a method of gatekeeping, or enforcing ways of how smart contracts are enforced dependent upon some organization politics. The governance aspect of any smart contracts is what needs to be deliberated upon in any operational thinking to understand how it is contingent, and not to allow trust.

Hybrid architectures attempt to mitigate the concern of actualization and verifiability gap by relying on dual-layer smart contracts in which the public smart contracts require that procedural milestones (e.g. contract award timestamps, delivery notifications) be enforced while internal operations are managed under the private smart contracts (e.g. bidder scoring algorithms, disbursement authorization). Diadia et al. (2023) illustrate how this type of hybrid smart contracts was employed in their deployment in Hyperledger Fabric for procurement dematerialization in which external stakeholders could verify key events on the public ledger while the related sensitive logic remained private. This design facilitates selective transparency while ensuring operational secrecy and confidentiality but again is reliant on the governance around who has rights to deploy contracts, amendment governance, and authority to resolve disputes.

Importantly, the literature has been clear to mitigate the risk of uncritical meant that smart contracts can indicate or defer to original governance (as in conventional procurement systems, where courts may override or impose rules) but as stated, smart contracts enforce predetermined rules at the time of execution with little to no human oversight or intervention. Other factors to consider are the opacity surrounding the implementation of contracts and whether the functions of the appointees you are laying down in your smart contracts would be similar to how a poorly regulated IERC contract ("Layer 2") would act or legitimized - a typical risk of hybrid smart contracts mentioned before. Carvalho (2019) and Bai, Zhang, Sang, and Liu (2022) urge for smart contracts

to have to be subjected to external review and included within a stupor for traditional accountability and oversight. This is even more beneficial in permissioned settings where there is collusion between validator's which is a transitive service and under-determined governance within privately established rules.

Consequently, smart contract innovation was followed through by on-boarding the workings of the contractual tie to type selection based on the understanding that even genuine innovation around smart contracts remain tied to typological choices. Public chains have an inclination towards open governance and rule-based enforcement, and issues of legal harmonization and institutional acceptance exist. Permissioned chains support operational choices and legal conformity but create situations for rule manipulation and selective enforcement. The literature suggests that the reasonable governance arrangement is one that embraces code-based automation with human scrutiny, legal assessment, and civic auditability based on the risks of corruption and maturity of the institutional context for procurement.

The selection of blockchain typologies for public procurement is not simply a matter of chosen technical architecture or functional design. It is shaped by the field of institutional trust, the strength of legal-administrative frameworks, and stakeholder incentives. These contextual elements help determine if a blockchain system is fully assumed as a transformative anti-corruption system or a digital upgrade that preserves the existing procurement status quo.

Institutional trust is significant in ambition for decentralization to which governments are prepared to accept. In high-trust contexts like Estonia or selected Nordics, public agencies are seen as reliable stewards of public funds and data. Governments in these contexts tend to see benefits from adopting permissioned blockchains as secure and auditable tools to build upon their embedded digital legacies (Sung & Park, 2021). In this formulation, a focus on the integrity of the data and resilience to tampering and unauthorized changes was more salient than an expectation of public transparency or civic oversight. In lower trust contexts where procurement is viewed as being open to elite capture or patronage, public or hybrid blockchains provide a potential method for outsiders to verify the procurement process, allowing civil society and the media to check reporting without formal investigative processes (Bolívar & Prados, 2022; Andrade et al., 2024).

Even so, public transparency mechanisms are subject to the reliance on surrounding legal and political systems. For example, if a jurisdictions access to information laws are weak, or courts do not recognize blockchain chain records as lawful, or procurement laws do not incorporate automated processes, it is unlikely that blockchain reform will generate reliable accountability. Carvalho (2019) evidenced this point in Italy by illustrating that technically sound permissioned blockchain deployments became trapped by institutional resistance and competing bureaucratic interests and did not produced change because there was a lack of judicial adaptation. Sánchez (2019) added to this discussion by advising that transparency is inadequate without institutional mechanisms by which government officials can act on the use of blockchain to identify

procurement irregularities, whether through institutional procurement courts, independent auditors infused with oversight authority, or meaningful repercussions to bad behavior.

Stakeholder dynamics affect typological outcomes to a substantial extent. For example, public blockchain adoption and implementation is often met with hostility because of the existing incumbent actors (i.e., procurement agencies, IT suppliers, or politically entrenched contractors) that understand decentralization and transparency directly threaten existing revenue models and discretionary power (Bai et al., 2022; Roeck et al., 2020). As such, a growing tendency towards public-sector procurers adopting permissioned blockchains often take precedence over public blockchains because a permissioned blockchain offers a more palatable, controlled nature of decentralization while allowing governments to promote being digitally modernized. However, Nodehi et al (2022) have suggested that co-optation is a real concern in such illustrated preference over public blockchains as public organizations assimilate decentralization into existing bureaucracies to bolster administrative controls. Blockchain may thereby provide mechanisms for expedient production and subscription within the existing hierarchical procurement landscape rather than the opportunity to address corrupt practices.

The resistance to decentralized arrangements is further implicated in political economy interests across digitally modernized procurement contexts. Brazil and Lebanon highlight the example of how powerful contractor cartels and politically connected elites make sense of institutional complexity to delay and/or modify blockchain implementations in ways more amicable to the impact of institutions (Mahmalat & Maktabi, 2023; Bolívar & Prados, 2022). When typologies are selected in such contexts, the decision often reflects not the technical appropriateness from a ranking but is a choice to respond to political pressure and manage reform aesthetics while preserving procurements capture.

The literature converges on a clear finding - typology does not indicate success or failure; it is the manner in which the chosen architecture interacts with institutional incentives, legal standards, and stakeholder configurations that contribute to success. Public blockchains may fail in a politically hostile environment devoid of legal supports. Therefore, permissioned chains can work provided there are strong accountability frameworks and transparency over governance. In a larger sense, the typology of blockchain being adopted should connect to a wider governance reform strategy that recognizes complementary issues of legal coherence and harmonization, institutional design, and participatory monitoring and oversight.

The preceding review indicates that through considerable affordances and constraints, public, permissioned, and hybrid typologies of blockchain are capable of responding to various types of corruption that accompany public procurement. These trade-offs are not just technical; they represent larger institutional, legal, and governance logics. Public blockchains offer the most transparency and decentralized enforcement but are generally burdened by legal ambiguity, scaling governance complexity, and political viability within most state systems. On the other hand, permissioned chains offer control over operations and some legal coherence but risk centralization,

limited auditing, and elite or ego capture and compromise their integrity-enhancing value. Finally, hybrid architectures attempt to mitigate the issues related to public vs. permissioned but are still under-theorized and context-dependent in terms of how they are applied or deployed in the real world.

The ambiguity of typology classes is particularly relevant to anti-corruption procurement reform where the connection between the affordances of blockchain functionalities and some corruption mechanisms is very important. For example, time-stamped and publicly verifiable auction logic may offer the most transparency for dealing with bid-rigging or collusive tendering issues—and be almost impossible to implement using permissioned or hybrid solutions. However, payment fraud or other post-award fraudulent manipulations may require permissioned systems that tightly interwoven with financial compliance frameworks. In fact, the authors identified little largely survey and literature-type documentation of how mechanisms map to typologies related to corruption, leaving implementations, suggestions, or decisions to previous generalities or vendor disposal. This absence of mapping offers a clear research contribution that this dissertation is directly influenced and applied to develop a procurement-corruption typology and compass offer in terms of concrete residual affordances of blockchain and corruption.

In addition, while lots of proclamations are made about potential affordances of blockchain-induced change, very few contributions have applied a tri-dimensional structure for governing blockchain as a reality in private or commercial use: legal, regulatory, and technological dimensions. As persuadable as illustrated through the adoption of a new procurement code in Italy, and through deploying regulatory sandboxing in Canada or inter-governmental fragmentation in the case of the US federal procurement system, appraising typology is rarely solely a technical decision. To a far greater effect, typology considers how national systems brokers transparency, discretion, innovation, and legal rigidity. This dissertation will use this dimension of interoperability to draw comparisons across three legal regimes (civil and common law), with particular focus on how typologies potentially interact with either domestic legal norms, doctrine of administrative law, or institutional workflows around procurement in those jurisdictional contexts.

This review has established the scholarly and policy urgency for typology-focused research relating to the mechanisms of corruption, which will arguably increase understanding of institutional logic and practices. The novel contribution of this focus is not to emerge with a single “best” kind of blockchain, but rather an analytical perspective to understand different typologies and what those affordances may mean for different anti-corruption outcomes under various institutional, legal, and regulatory constraints. This will also directly support Hypotheses 1, 2, 3, and 4 in this dissertation, and expand a platform to achieve Objective 3 and Objective 4.

In summary, typology should not be seen as a static classification, but as a normatively flexible governance choice that must be construed by the corruption vulnerabilities it intends to limit, the institutional faculties it works within, and the social and legal readiness of the procurement field.

It is this complexity that must be considered in evaluating the anti-corruption potential of blockchains—not as a one-size-fits-all vehicle, but as sophisticated and malleable tool that is contextual in borders and could be specified as much upon governance and legal legitimacy as it is about the technology.

2.2.2 Risks and Challenges of Blockchain Implementation in Public Sectors

Although blockchain may hold valuable promise in enhancing the transparency, accountability, and efficiency of public procurement systems, an emerging number of studies are discovering a range of risks around its adoption in practice. These risks are not limited to technical concerns, but are extended through legal, regulatory, organizational, and sustainability issues that are all connected—challenging the overall institutional fit of blockchain in government systems (Batubara & Janssen, 2018; Cagigas et al. ,2021; Sousa, 2023). Accordingly, while it is true that early anticipation of blockchain's optimistic potential often emphasized blockchain's prospect of eliminating a well-established history of corruption and lack of accountability in government bureaucracies, much more recent evaluation of blockchain has re-iterated the point that blockchain is inherently neither truly neutral or universally benevolent. Indeed, the implementation of blockchain must consider contingent vulnerabilities which, if not appropriately contextually managed, may replicate or exacerbate the very governance failures the technology is intended to address (Tan, 2023; Curry, 2024).

The most often cited critique considers how technical centralization, or governance by few, undermines public systems with solutions based on permissioned and/or consortium blockchains used in public sector applications. While large distributed pools of validator nodes are useful in public administered blockchains such as Bitcoin or Ethereum, in government acquiesced blockchains consensus is usually relied on a small group of pre-chosen actors or nodes (Sedlmeir et al., 2022). This can lead to collusion of validators regarding transaction ordering, loss of updates, or collated activity within special interest or cartel-like behaviors (Esposito et al., 2025; Dziundziuk and Dziundziuk, 2022). The presence of asymmetries in authority or institutional capacity, for example, undermines the concept of decentralization and likely creates levels of public distrust, and erodes resilience by introducing additional vulnerabilities into systems (Batubara & Janssen, 2018). Further, the design of government blockchains can reinforce bureaucratic or political power structures and hierarchies under the guise of technology, by what some have called 'governance opacity by design' (Sousa, 2023).

The risks expressed above are compounded in institutional settings that have experienced or have a history of institutional capture by civil servants or cadre capturing of procurement processes. To that end, there is little replacement for ground knowledge regarding the boundaries concerning discretions of civil servants in procurement processes. In this way, postal and curatorial changes to technologically-centralized blockchain support will likely only tokenize, not dismantle longstanding traditional power asymmetries (Curry, 2024; Rana et al., 2021). Related, without

robust oversight frameworks there is a risk that consortium chains would be operated by dominant actors (e.g., ministries or contracting agents), who embed their interests in consensus protocol and undermine accountability, which was objectively designed to support productivity improvement (Tan, 2023; Dziundziuk et al. 2025).

An equally relevant barrier is that of operational resilience, whereby organizations experience a continuous process during failure (point) events or failures to draw on their organizational capabilities. While decentralized infrastructure generally produces a highly distributed structure from their protocol (blockchain architecture) (Sedlmeir et al., 2021), many, if not most, government-attributed cases are exposed to localized infrastructure outages/interruptions, vendor misconfigurations, or administrative gates (Malik et al. 2021). Bottlenecks typically occur at local nodes in the network, and can result from conflation of limited-service players, or administrating only closed-source platforms which limit multilateral performance for distributed network nodes-redundancy, or inability for many-associative (blockchain syntax) failover in public sector ontology (Monrat et al., 2019; Sanka et al., 2021). Moreover, if the government applications are nested within public procurement processes which include multi-jurisdictional governance challenges—particularly in large countries possessing complex associated jurisdictions—these examples of infrastructure fragility will be further amplified in processes of institutional silos. An example in the Canadian contextual orders, the prospect of reducing silos in federally policed public procurement challenges is lessening through newly understood shared digital infrastructures.

Ultimately, although the ideal of decentralized governance is an important aspect of blockchain theory, the real-world situation in public sector environments shows a continuing tendency toward the centralization of technical and administrative functions of centralization. This dilemma requires not only technical redesign but also a reconceptualization of the institutional logics and accountability frameworks that shape public sector innovation. Failing to recalibrate will result in the continued shortfall of blockchain-based anti-corruption behaviors to take promises to fruition, overshadowed by the new risks that changing reform architecture presents.

In addition to technical centralization, a significant challenge is the rigidity and legal ambiguity of smart contracts in public systems. Smart contracts are shifted to self-executing code within blockchain technologies that automates transactional operations based on mutually predetermined conditions, offering operational efficiency by removing intermediaries and de-intensifying discretion (Wang et al. 2019). The deterministic nature of their operation limits their usefulness to apply to public sector environments, where ossified legal and procedural diffusions require flexibility, interpretability, and dispute resolution (Shermin 2017). Unlike traditional legal contracts that could be contested and interpreted with contextual meaning, smart contracts are simply coded processes lacking semantics and specific contextual detail—making them wholly inadequate to capture public procurement law or the judgements of discretion exercised by administrative decision-makers (Liu 2021).

Literature has begun raising concerns about the use of smart contracts in legal–institutional settings, especially in their underdeveloped potential to deal with unforeseen circumstances, negotiations of contracts where circumstances have changed, and the regulatory change associated with infrastructure changes that smart contracts and blockchain will likely bring to public sectors. Zamani et al.In their scholarship, Allgood & Staab (2018) suggest that the immutable nature of deployed smart contracts, while helpful in establishing integrity, is fundamentally problematic when public entities require legal reversibility—particularly in instances of fraud, system failure, or non-compliance. The lack of a capacity to change a smart contract at all is especially problematic in a context of administrative law where an agency at least needs the discretion to unmake a decision to adapt to a shifting public interest or procedural fairness. As Shu et al. (2021) describe, the absence of standardized rollback processes, or any sort of override capability, introduces serious governance and liability issues, especially when the execution of a algorithmically enforced smart contract has the potential to undermine constitutional or statutory obligations.

A related issue of legal non-repudiation is also unresolved in most jurisdictions. Blockchain records are tamper-evident, but existence of a transaction on-chain provides no assurances of legality or enforceability in cases where prohibitions are not established by domestic law - and this hurdle has no legal precedent regarding its establishment in law across most legal systems (Yu, 2024).This creates a precarious area of ambiguity where the public actor may very well be acting under a smart contract, but without the necessary statutory authority, and thus, open to litigation and robbing procedural legitimacy (Padmanegara et al., 2023). The issue of the problem becomes compounded if the contract code was commissioned or developed by a third-party provider who has not made reasonable attempts to legally validate the governing code, and there are risks of algorithmic execution that operate directly contrarily to any of the procedural or administrative rules that are outlined prior to adoption (Sousa, 2023).

The rigidity and hardness of smart contracts also generates a set troubling questions around equity and accountability. In high-stakes public procurement implementations—especially injections into infrastructure or healthcare provisioning—the inability to pause, change, or terminate the execution of a contract based on new evidence or social need could create results that, while legally binding, are substantively unjust (Shermin, 2017; Curry, 2024). This disjunction between legal form and public interest raises the question of techno-legal harmonization: where automation can reasonably be applied, legal boundaries and institutional oversight mechanisms are also critical to ensure substantive justice.

While some combinations of off-chain adjudication and on-chain enforcement as hybrid architectures have been suggested to ameliorate some of these tensions, there is a limited amount of empirical validation for these claims. Wang et al. (2019) refer to a number of experimentally designed iterations that combine judicial review or fallback clauses or reconfigurable modular smart contract building blocks—but most haven't been built into government systems at scale. Further demonstrating the gap between conceptual design and institutional adoption, there

remains a need for a normative and regulatory infrastructure that allows for the benefits of automation while simultaneously allowing for the integrity of law.

There is another layer of complexity associated with blockchain adoption in the public sector, arising from conflicts around jurisdictional data privacy and records keeping practices; more specifically, with respect to the immutable and documented historical records on blockchain ledgers and the obligations imposed by legislative frameworks such as the General Data Protection Regulation (GDPR) to delete information. The blockchain data governance architecture is append-only, which is crucial to the aspirational integrity and traceability of records, though introduces a fundamental incompatibility with rights-based data governance paradigms that have established arrangements for individuals in relation to the control of personal data (Akanfe et al., 2024; Bernabe et al., 2019). The incompatibility is more acute in public administration, where governments have legally mandated (or required) protection and potential erasure of sensitive personal information about citizens, applicants or contractors.

The "right to erasure" granted to individuals under the GDPR in Article 17, enables data subjects to request the deletion of personal data from information systems under certain circumstances. However, deleting information that has been recorded on a blockchain, notably from public/blockchain records and under commonly distributed ledgers, is technically infeasible in ways that would not undermine the "integrity" guarantees (Kshetri, 2017). There have been limited successes in ways to get around GDPR compatibilities-related to appropriately removing the personal identifiers from on-chain and pseudonymizing personal data, with a great deal of legal uncertainty surrounding these recent experiments (Bodó and Janssen, 2022). While it may be possible to store personal data off-chain and deploy relevant hash pointers on-chain for public records use to mitigate direct violations, regulators are uncertain whether how the blockchain structure removes the traceability of personal identifiers from the record, as it relates to being combined with other relevant data sources (Wylde et al., 2022).

These legal-tech frictions are the basis for an ever-increasing volume of academic literature critically analyzing the challenges of developing privacy-preserving solutions to foster compatibility for the durable document features of blockchain with data-privacy policies. Specifically, Bernabe et al. (2019) discussed zero-knowledge proofs, homomorphic encryption, and differential privacy as a means to minimize exposed data when it was presented on-chain. While these ideas look exciting on paper, they present potential impediments to implementation at scale in real-time public-sector systems with respect to computational resources and standards. In parallel, there are also proposals for unevenly implemented governance through permissioned architecture so that there are governance arrangements with good access (Toufaily et al., 2021), yet such architectures introduce complex issues around centralization and exclusion that have already been discussed.

Jurisdictional fragmentation exacerbates these challenges. In federal systems like Canada or the United States, data protection laws may differ at the provincial or state level, removing the ability

to deploy block chain solutions with uniformity across geographical demarcations (Tan, 2023). A legal requirement that is completely compliant in one sub-national region IM may not legally fit in AM; therefore, interoperability is compromised and litigation/regulatory risk increases. Furthermore, with cross-border procurements, or international aid contracts — circumstances that could embrace the transparency of chain of block if adopted — lack of harmonized privacy standards is a key hurdle to uptake.
Moreover, this tension relates not only to the legal or technical level but also conceptually. Sousa (2023) contends that privacy frameworks and blockchain technology exemplify fundamentally different constructs of trust because blockchain technologies rely on technological immutable and distributed verification, while trust in privacy frameworks is purposefully constructed through autonomy, reversibility and consent. Getting to the other side of the above construct will require more than just technical "patches" and will entail a fundamentally interdisciplinary reconsideration of the ways that public institutions will structure, govern, and steward sensitive data in a digital world.

The issues of environmental sustainability and computational scalability have also become salient issues in assessing the ability to deploy blockchain technologies in the public sector. Although the issues of energy and computational overhead are typically associated with first-generation, proof-of-work (PoW)-based block chains, like Bitcoin, the broader implications of energy consumption and computational overhead are present in across blockchain architectures and use-cases. In the case of public procurement and public governance (information systems), where efficiency, cost-effectiveness, and environmental responsibility are crucial, these issues are large hurdles to the mainstream uptake (Min, 2019; Saberi et al., 2018).
Public blockchains employing energy-intensive consensus mechanisms have attracted much unwelcome scrutiny for their relative environmental impact. Upadhyay (2020) observes that PoW networks can consume more energy than some nation-states, and for public institutions with sustainability mandates PoW-blockchain networks are often hard to justify. This sustainability burden potentially undermines the 'green transition' ambitions being touted by governments (especially in styles like the EU and Canada), and also creates reputational and ethical risks for public institutions pursuing blockchain solutions if there are no attendant mitigation strategies put in place. Even in the slower energy consuming ecosystems of permissioned blockchains, or proof-of-stake (PoS) alternative, the concerns over scalability often remain, especially in simultaneously fast-paced use cases such as real-time procurement auditing, or identity verification of contractors or individuals across multiple agencies (Monrat et al., 2019).
The scalability dilemma refers to a blockchain's capacity to handle only large amounts of transactions, but the transactions need to be processed with a low-latency and low-cost. This is particularly relevant in public systems where speed and accessibility are imperative to being public-sector friendly to blockchain solutions. Batubara et al. (2019) conducted a comparative analysis and highlight that many of the pilot projects trailed in public administrations reveal issues to do with throughput bottlenecks. This throughput issue ultimately hurts the speed of service

provision in some instances, slow the quers, timeliness of bid processing; ultimately reducing trust and interest from end-users. These issues do not only highlight a problem with technical application of blockchains in public administration; not being able to process Procurement bids, on a transparent system, through a timely mechanism, may create new inefficiencies rather than solving any inefficiencies (Cagigas et al., 2021).

Moreover, scalability challenges often combine with other risks considering governance complexity and vendor lock-in. As agency needs grow, public sector agencies, as a matter of necessity, may transfer governance and operational accountability to private vendor(s), or access vendor-related proprietary layer-2 scalability. Risks regarding performance are likely to intensify challenges to lock-in, opacity and loss of agency governance accountability that accompanies governance and operations and cognitive inertia (Dziundziuk et al., 2025). Even if outsourcing is critiqued primarily on performance grounds, rather than expedience, agency governance in scale and complexity is compromised if agencies have no reasonable chance of internal oversight over technical realities (Sanka et al., 2021).

While a number of newer types of consensus mechanisms—including Byzantine Fault Tolerant (BFT) protocols or Directed Acyclic Grahps (DAGs)—are promising in terms of scalability or energy-related issues, their maturity and interoperability remain limited, especially in the context of public sector engagement (Saberi et al., 2018). In relative terms, a considerable gap exists in a lack of standard benchmarks for identifying appropriate measures for assessing performance against other options in government environments. As such, principal concerns about energy consumption or scalability - should not be perceived as sole performance measures, but rather considered as systematic inhibiting performance measures risks that overlap governments environmental policy, fiscal management, and agency capacity.

One additional challenge, which may not be as distinctly visible as vendor lock-in through technical governance dependencies and opacity exists with risk of technical lock-in - that is, not only is blockchain purportedly transparent but also obviates responsibility and accountability because of acceptable obscurantism through interconnected tool-chain complexities (Sedlmeir et al., 2022; Sousa, 2023). The complexities of adopting blockchain in any government-type context can implicitly set unforeseen technical dependencies in place that increasingly exacerbates opacity in terms of decision-making processes; layering in technical circumstances that will be unmanageable.

Technical lock-in is normally identified when the public-sector organization becomes structurally dependent upon a vendor or specific protocol development consortium to work or upgrade the system (Dziundziuk et al., 2025). More often than not, dependencies exist with proprietary codebases, non-standard based or agreed interfaces, or operational conditions built from service-level agreements which hamper administrative governance flexibility. Dependency fades over time either with slow decisional inertia towards continual investment, or shows increased removed

capacities within the agency, such that scale or complexity becomes near impossible, with decreased operational capacity to engage in overall or systemic digital policies or services ecosystems - creating barriers for future service access and resulting in increased costs for future procurement actions (Malik et al., 2021). Depending upon the type of government framework, or the disruption of either a federal and/or jurisdictional context engaging in technical-disruption, the limitations of architectural rigidity, and control from contractors in contemplation of overall policy structures creates issues of digitally resultant capability which threatens inclusion strategies or evolvability

Lock-in whereby both the derivation of a capability and functions based on data structures via contracts can intervene in observable procurement agreements at a technical protocol, specifically when smart contract logic or data schemas are grounded in an immutable ledger, is also seen (Rana et al., 2021). Either situation means outcome/behavioral assumptions in public sector operations are underpinned in a set of contingencies around when the level of complexity generates costs with only a minor change in policy direction or regulation - leading either too costly system replacements or the generation of an entirely new parallel chain, resulting in contingencies not merely focused on costs or operational risks but as tacit prospects for policy inertia, legal liability or disdain of policy reform - essentially everything a technology was theorized to expedite (Toufaily et al., 2021).

Moreover, the opacity of governance occurs when decision rights in blockchain systems - who can validate, who can shift permissions, or who can alter code - are poorly specified, and not democratically accountable. Esposito et al. (2025) state that while the end goal of decentralization is a normative concept, governance in blockchain-based systems, if it even exists, is poorly specified and governed by a limited number of technically competent actors. This asymmetry may confirm existing bureaucratic hierarchies, or allow for technocratic state capture, where essential design and policy tasks can be made without public attention, scrutiny, deliberation or accountability (Tan, 2023). In addition, the governance arrangements of consortium blockchains create space for decision-making opacity based on opaque inter-agency agreements (or memorandums) or informal negotiations that exclude audit engagement - with either users or civil society - to understand who does or does not have operational decision making and accountability roles.

The non-substantive threats to transparency or integrity of decision-making process are not meaningful arguments on a board; early deployments of blockchain in the public sector have also demonstrated movement from original governance principles of transparency and decentralization when they do not meet the needs of convenient or even enforced administrative or vendor control (Sanka et al. 2021). Governance drift demonstrates the potential system vulnerabilities that exist in all institutions willing to privilege technological possibilities over legitimate democratic expectations of accountability, particularly in contexts with different levels of access to digital literacy or regulatory capacity (Cagigas et al. 2021).

So addressing the possibilities offered by lock-in and opacity with blockchain means that planners require not only technical progressive protections in the forms of open standards, auditability, or modular design, but substantive process norms and institutional instruments/practices that create opportunities for flexibility, inclusiveness, and transparency regarding system governance. Otherwise, like all projects, blockchain will begin to replicate the same pathologies of opacity and inertia that it sought to mitigate.

In combination the five complexity types - technical centralization, smart contract rigidity, conflicts in data jurisdiction, energy/scalability limitations, and lock-in and governance opacity - create an evolved and multi-dimensional risk constellation for blockchain systems in the public sector to navigate. Ultimately while each problem has surgical literature addressing it in isolation of the other problems, having as many risks as possible to contend with in their aggregated or co-operative forms becomes overwhelming if you begin to consider the reckless and legally obscure complexities that exist across distinctively politically plural settings like Italy, Canada, and the United States. The cluster of layered structural governance in which there are different agencies, different levels of government and different levels of regulation for pluralistic jurisdictions adds onto the vulnerabilities that have become universally evident in the literature and layers institutional readiness, intra-agency coordination and legal harmonization onto each and every planner's shoulders.

A common thread across this synthesis is that when deploying anything, you cannot extract it from the institution/legislative context it co-exists within. As Sousa (2023), and Sedlmeir et al. (2022) when use continues to be constrained even if follower agencies are willing to use blockchain to create transparency and decentralize processes, the agency can slip back into either opaque or imbalanced power norms very quickly and without changes to its institution. Likewise, many of these technical conditions for wait, "unintended" centrally governed blockchain systems in early adoption public sector literature demonstrate themselves when you realize existing design options for public processes do not come from the inherent expectations of blockchain; they originate from bureaucracies and security exacerbated inter-organizational negotiations even if they are more desirable (Batubara & Janssen, 2022; Dziundziuk & Dziundziuk, 2022). While the hypothetical benefits of adopting blockchain technology and the practical tensions will always be at odds, they risk undermining not only the legitimacy of governance processes but the legitimacy of the public's trust in the technology.

Additionally, the inflexibility of smart contracts and the open questions related to legal non-repudiation highlight that there is more than just drawing a logical legal conclusion that can then be coded. As scholars like Zamani et al. (2018) and Wang et al. (2019) note, moving from the public to automation requires more than simply technical feasibility, but a formal legal agreement, dispute resolution processes, and design features that will allow for discretion, unlike most administrative law. This is especially important in a public domain of procurement and contracting that may include exceptions, force majeure clauses, or discretionary provisions that cannot easily be represented in executable logic.

The ongoing conflict between blockchain immutability and the GDPR's "right to erasure" can also be seen as a consequence of the underlying ontological divergence between traditional data protection law and the design of distributed ledgers. The continued clash represents the long history of legal scholarship explaining the issues raised by blockchain technology, as well as the legal and technical attempts to partially resolve these issues, but it is now time to explore in greater depth fundamental regulatory innovation to address the incompatibility of these two paradigms. As noted by Bernabe et al. (2019) and Akanfe et al. (2024), achieving a workable resolution to this disparity may require legal innovations in concepts of erasure, anonymization, and accountability in light of nascent technologies, rather than forcing blockchain technology into existing outdated legal paradigms.

Likewise, the environmental and performance considerations of blockchain also create a policy problem that extends beyond technical issues. If governments want to use the blockchain for public good, especially for procurement systems that promise anti-corruption or efficiencies, then there needs to be considerations of trade-offs. In situations where a blockchain system improves transparency but increases carbon emissions or operational costs, any trade-offs would need to rely on public value frameworks that are clearly articulated, yet do not exist in most of the pilot studies or review articles contained in the literature review, confirming the gap between technical design and normative justification (Monrat et al., 2019; Saberi et al., 2018).

Ultimately, the risks of lock-in and opaque governance arrangements demonstrate that blockchain adoption can restrict institutional adaptability and threaten democratic accountability. As argued by Esposito et al. (2025) and Tan (2023), absent mechanism for purposeful institutional friction or participative governance approaches, blockchain may be reduced, by a limited number of actors, to a technocratic tool, not a collective empowerment tool. This is particularly problematic in contexts that are characterized by regulatory capture or institutional fragmentation—both common to the public procurement systems in the jurisdictions examined above.

Rather than simply identifying burgeoning levels of uncertainty and varying tensions, this synthesis reveals broader, ongoing tensions that are not simply characteristics specific to the initial adoption of new technologies, organized in a particular context, but are part of a larger political economic discourse of digital governance. For example, a continuing dilemma around transparency and privacy is shown in the literature. Transparency and privacy are framed as perpetual and unresolved paradoxes. The potential for verifiable audit trails and immutable record keeping—the hallmark of blockchain and often lauded as an anti-corruption or procurement integrity tool—are fundamentally at odds with conventions of data protection, such as the right to withdraw, erase, or amend one's record (Bodó & Janssen, 2022; Wylde et al., 2022). Addressing this dilemma cannot be done solely through a technical fix. Although workarounds, such as keeping data off-chain or using selective disclosure protocols (e.g., zero-knowledge proofs), have been used to mitigate risks, it is not clear they will avoid objection or enable processes, or even be operationally feasible, for many public sector organizations (Bernabe et al., 2019; Akanfe et al., 2024).

A second important contradictory observation relates to decentralization versus centralized implementation. Governments, with a vested interest in managing integrity of their systems, establishing legal compliance, and protecting the security of their operations, often adopt a permissioned or consortium blockchain implementation approach. Such approaches could produce tension for plausible governance reasons, but they also re-introduce centres of authority and could even technically collude or become entrapped by validator nodes (Esposito et al., 2025; Dziundziuk & Dziundziuk, 2022). The literature suggests that these tensions rarely, if ever, are acknowledged in formal project documentation or public debate or discussion—resulting in overstated descriptions about decentralization and, perhaps, downplayed risks of structural dependency (Sedlmeir et al., 2022). This reinforces what has been called an epistemically opaque governance context from a lack of democratic oversight and technical darkness.

Additionally, the public-sector literature on blockchain has demonstrated fracturing based on research discipline. Legal scholars often focus on studies of compliance and the enforceability of contracts, while computer scientists focus on consensus algorithms, cryptographic techniques or system performance, and in most instances, public administration academics focus on or explore subjects of organizational fit and policy innovation. Although many of the above samples are of great significance, few studies consider how to integrate the informatics, law, and organizational elements to present a holistically articulated picture of the socio-technical risks associated with public sector contexts for blockchain (Sousa, 2023; Rana et al., 2021). Policy cannot meaningfully escape blind spots or mistakes in or of either discipline, where, while technical solutions are potentially developed with an insufficient consideration of legal doctrine or an institutional capacity, or vice versa.

The lack of empirically backed research on a grand scale also limits the explanatory and predictive power of the literature. As noted previously, while there are numerous articles that apply systematic reviews or conceptual frameworks (e.g., Batubara & Janssen, 2018; Cagigas et al., 2021; Toufaily et al., 2021), there are no longitudinal, multi-jurisdictional case studies that examine how blockchain risks develop over time and across different legal and administrative contexts. For example, Italy has experimented with blockchain technology for anti-corruption platforms through ANAC pilot programs, and Canada (along with some provinces) has piloted blockchain technology in supply chains and identity services, but evaluations remain rare and lack generalizable theory (Malik et al., 2021; Dziundziuk et al., 2025). Without these kinds of studies, it is extraordinarily difficult to generalize best practices or project unintentional consequences of design decisions made in a complex public procurement setting.

Also of note is that, as Upadhyay (2020) and Sanka et al. (2021) highlight, the literature seldom engages with political economy factors—such as lobbying from technology vendors, institutional inertia, or policy cycles—that can ultimately shape the trajectory for blockchain adoption. This is particularly troublesome in the public procurement space because of the existing vested interests and structural inefficiencies that resist change, and the absence of this political economy consideration has the potential for blockchain to be framed as a neutral, exogenous innovation

instead of the contested technological innovation that it truly represents, contingent on space, place and power, regulation, and accountability. Given the multiplicity and complexity of identified risks, it is unsurprising that the literature also indicates some important research gaps—most importantly, in relation to empirical validation, regulatory congruence, and inter-contextual learning as vital conceptual models and technical recommendations continue to proliferate, few have devoted any systematic attention to empirically validating their practical applicability in actual public procurement systems in a diverse range of jurisdictions (Cagigas et al., 2021; Bernabe et al., 2019). As a result, we have a rich theoretical landscape of research possibility but empirical data does not enable us to generalize with confidence in environments as disparate in legal and institutional forms as Italy, Canada, and the United States.

First, there is a lack of empirical studies in the area of technical centralization that examine how validator governance, delegating consensus, and node permission variables evolve in public blockchain sustained over time. Although authors such as Dziundziuk & Dziundziuk (2022) and Esposito et al., (2025) identify structural weaknesses in consortium-led architectures, few studies analyze whether they lead to inconsiderable divergences from stated decentralization principles or structured collusiveness in practice. There is also hardly any research on the types of institutional conditions, if any exist, that encourage or endorse centralization, rather than decentralization - for instance when it comes to national security, cross-border date compliance or inter-agency rivalry (Sedlmeir et al., 2022).

Second, there is a lack of doctrinal studies examining how various jurisdictions apply validity and legal non-repudiation to code-based contracts in an administrative or procurement capacity. That some jurisdictions have begun recognizing smart contracts through statutes structuring the formation and enforcement of these contracts in a commercial context (certain U.S. states and the UK), public sector applications implicate different degrees of legality, procedural fairness, and constitutional audit which is barely covered in our literature (Shermin, 2017; Liu, 2021). We also lack comparative legal scholarship which examine how jurisdictions with different legal forms characterized by different dominant legal traditions (i.e., civil law in Italy, common law in Canada and the U.S.) will determine outcomes from smart contract disputes, overrides, or regulatory interventions. The above body of legal research is important for developing implementation strategies based on the robust legal basis which complement a sound technological basis (Yu, 2024).

Third, jurisdictional conflict around data privacy, e.g., GDPR and immutability of transaction data, has been heavily theorized but has received very few empirical studies evaluating operations in practice. As Akanfe et al., (2024) and Bodó & Janssen, (2022) point out, those theoretical recommendations—such as selective disclosure, and a mix of on-chain and off-chain data stored—have never been investigated in real-world government systems. Moreover, it is unclear how regulators, data protection agencies, or courts 'read' these types of technical solutions into existing law. For example, given that the GDPR allows for hashing personal data off-chain, and storing references to that data on-chain, it is unclear if that practice is considered effective

pseudonymization of personal data, or if identification still remains possible when combined to auxiliary datasets (Wylde et al., 2022).

Four, in the context of energy consumption and scalability, many technical assessments rely on simulation or benchmarking from private-sector platforms rather than direct assessments of blockchain applications in public service settings (Monrat et al, 2019; Upadhyay, 2020). There are few lifecycle cost assessments or carbon emissions assessments specifically related to the use of blockchain in regulatory or procurement systems. In addition, there is also no standardized approach to evaluate the trade-offs between blockchain's transparency benefits versus environmental externalities in the public sphere, which bounds the ability of policy actors to make the best possible decisions that support sustainability goals (Min, 2019; Saberi et al, 2018).

Lastly, in the context of technical lock-in and governance ambiguity, research almost always stops at problem identification. While scholars have clearly articulated the risks of vendor lock in, proprietary protocols, and non-democratically sanctioned design (Tan, 2023; Sanka et al, 2021), there is very little scholarship on mitigation strategies. At the same time there are virtually no empirical cases dealing with open-source governance models, participatory design approaches, and modular implementations that can be co-developed with end users in the public sector. Absent that, the normative promise of blockchain as democratic agent at the same time risks succumbing to institutional stability and politically induced inertia.

These knowledge gaps are not simply distinctions of the academy; they reflect strategic gaps in the sustainable transformation of public institutions. These gaps will require not only interdisciplinary research but also collaborative agreements between technologists, researchers, public administrators, and policy actors. A commitment to evidence-based development, transparent evaluation, and normative comparison will be necessary for harnessing the public value of blockchain while reducing the established risks identified in the academic and practitioner literature.

To provide a more structured understanding of the gaps indicated by the literature, Table 2.2.2.1 below provides a Research Gaps Matrix to plot each risk domain against four areas of academic underdevelopment: (1) empirical case studies, (2) legal and regulatory analysis, (3) technical solution validation, and (4) governance model evaluation. The matrix summarizes findings from the sampled sources and illustrates where the academic conversation has produced the most academic literature and where it has produced the least.

Table 2.Table 2.2.2.1 — Research gaps across blockchain risk domains (public sector)

Risk domain	Empirical case studies	Legal / regulatory analysis	Technical solution validation	Governance model evaluation

Technical centralization	Moderate	Sparse	Moderate	Moderate
Smart-contract rigidity	Sparse	Extensive	Moderate	Sparse
Privacy / GDPR clashes	Sparse	Extensive	Sparse	Sparse
Energy & scalability	Sparse	Sparse	Moderate	Sparse
Lock-in & governance opacity	Sparse	Sparse	Sparse	Sparse

Note. “Extensive” = active, well-developed literature; “Moderate” = growing but limited; “Sparse” = critical gaps. The scarcest area across domains is governance model evaluation, especially real-world validator design, accountability, and exit strategies.

Interpretive notes and academic rationale

Technical centralization (Moderate / Sparse / Moderate / Moderate). The empirical record on permissioned and consortium blockchains in public administration is emerging but uneven—case material exists for pilot systems and narrow deployments, yet generalizable findings remain limited. Legal analysis is comparatively sparse because most doctrine addresses data protection and evidence rather than validator governance or quorum rules. Technical mitigation patterns (e.g., PBFT configurations, public-hash anchoring, independent oversight nodes) are described in the computer-science and information-systems literatures, warranting a ’Moderate’ score for solution validation. Governance model evaluation is also ’Moderate,’ reflecting conceptual frameworks for consortium design but few audited, real-world governance reports.

Smart-contract rigidity (Sparse / Extensive / Moderate / Sparse). Legal and doctrinal work on enforceability, reversibility, proportionality, and administrative review is substantive and comparatively well developed (e.g., compatibility with public-law principles and procurement remedies), hence ’Extensive’. Empirical case studies remain ’Sparse’ because production-grade public deployments with jurisprudence are rare. Solution validation is ’Moderate’: formal verification, upgradeable proxies, and human-in-the-loop controls are established technically, but their translation to administrative procedures is uneven. Governance evaluation is ’Sparse’, as institutions rarely publish override protocols and appeal pathways for automated acts.

Privacy / GDPR clashes (Sparse / Extensive / Sparse / Sparse). Data-protection analysis is ’Extensive’, particularly on Article 17 (erasure), controllership, and pseudonymization under GDPR. Empirical evaluations in government settings are ’Sparse’; most evidence derives from proofs-of-concept rather than live systems serving citizens or vendors. Technical validation is ’Sparse’ because privacy-preserving cryptography (e.g., zero-knowledge proofs) and off-chain/on-chain architectures lack standardized, at-scale implementations in procurement

portals. Governance evaluation is ’Sparse’ given the absence of published DPIAs, regulator determinations, or standing operating procedures for handling erasure and data-subject rights within blockchain workflows.

Energy & scalability (Sparse / Sparse / Moderate / Sparse). Public-sector specific life-cycle assessments and carbon accounting remain ’Sparse’, as do legal analyses that integrate sustainability mandates into procurement technology choices. Solution validation earns ’Moderate’ based on tested alternatives (PoS/BFT consensus, batching, and Layer-2 approaches) that improve throughput while preserving auditability. Governance evaluation is ’Sparse’ because few institutions specify performance SLAs, fallback modes, or escalation paths that connect system capacity to statutory deadlines (e.g., bid-submission windows).

Lock-in & governance opacity (Sparse / Sparse / Sparse / Sparse). Across all quadrants this domain is underdeveloped. Peer-reviewed case studies of vendor exit, portability, and interoperation in government blockchains are rare. Legal analysis seldom addresses contract clauses for source-code escrow, change-control rights, or portability tests. Technical solution validation is limited for open-standards conformance and modular migration paths. Governance evaluation is scarcest: few deployments document validator selection criteria, quorum thresholds, upgrade procedures, or independent audit access in a form that allows scholarly assessment.

Ratings synthesize peer-reviewed studies, systematic reviews, and grey literature on public-sector blockchain deployments. They are conservative and oriented to procurement use-cases. ’Extensive’ indicates a mature body of scholarship with convergent findings; ’Moderate’ indicates active, growing work with partial validation; ’Sparse’ indicates critical gaps where conclusions would be premature. Section 5 operationalizes these gaps into testable propositions and evidence requirements for the comparative cases (Italy, Canada, United States).

This table suggests that legal and regulatory analysis received relatively complete treatment in the areas of enforceability of smart contracts and data privacy, which can be attributed to the EU in regard to GDPR (Akanfe et al., 2024; Liu, 2021). However, there were no empirical case studies to substantiate theoretical claims, or inform best practices regarding implementation - at least with respect to all five areas we identified no documentation regarding the energy impacts involved, and how systems were governed in actual public deployments (Monrat et al., 2019; Cagigas et al., 2021). Next to empirical case studies, there was moderate treatment of the technical solution space, especially as based on the proposals of cryptographic privacy mechanisms, alternative consensus approaches, and layered architectures. However, these studies were usually proofs of concept or simulation-based studies and did not demonstrably show implementations or policy pathways (Bernabe et al., 2019; Wang et al., 2019). The weakest domain - taking all areas into account - are governance models studies, especially studies that examine who, in practice, is exercising governing authority over these systems, if authority is delegated or co-shared, how decisions rights are shaped by institutional norms and user expectations and, ultimately, system legitimacy (Esposito et al., 2025; Tan, 2023).

Importantly, while each cell of the matrix highlighted a gap in each area of thematic inquiry, those gaps are related. For example, the lack of governance model evaluation in the context of technical lock-in, also brought to light the legal grey areas and accountability difficulties of smart contracts becoming automated (Shu et al., 2021). Furthermore, without empirical examinations of privacy-preserving solutions there are few mechanisms for regulators to independently evaluate any GDPR-compliant blockchain approach (Wylde et al., 2022; Bodó & Janssen, 2022).

The implications of gaps is significant. Absent any coordination of research across an empirical, legal, technical, and any institutional lens, governments may pursue not just blockchain solutions that are worse than their previous systems, but systems that further exacerbate admin fairness, citizen rights, and accountability for public expenditure. With respect to both doctoral research proposals, and future use for public innovation policies, the matrix serves as a guide for institutional and academic priorities in the near-term future.

The overlap of technical, legal, and institutional risks inherent to the implementation of blockchain in public procurement systems suggests the need for a precise research agenda that will produce tangible responses to unanswered questions across all areas of inquiry considered. Building off the matrix format and limitations articulated throughout this review, the following questions are presented as potential research directions for studying both policy and scholarly inquiries in relation to blockchain systems in the future. These questions represent academic blind spots and they are well-positioned in alignment with jurisdictional considerations required for cross-border implementation of blockchain systems in Italy, Canada, and the US. Each jurisdiction has a wealth of legal traditions, regulatory context and institutional capacities across levels of government decision-making within their jurisdiction.

1. In what ways might public sector blockchain systems be designed to reduce technical centralization and validator collusion without sacrificing efficiency or legal supervision?

This is a central concern in balancing the promise of theoretical decentralization with the requirements of institutional control in government systems. The literature has not yet provided ontologically understood governance designs which have achieved mitigation of the risks described above without a profusion to administrative opaque (Esposito et al., 2025; Dziundziuk, Dziundziuk, 2022), but does point to concerns with permissioned block chains and concentration of validators. With respect to procurement contexts - notably, phases of development of procurement in Italy's minimal codes administrative environment and divided decentralized procurement in Canada - this question requires comparative institutional analysis and audits in terms of their respective systems.

2. What are the legal and procedural frameworks necessary for enabling smart contracts that are enforceable, reversible, and adaptable in public procurement?

Smart contracts raise legal concerns of rigidity within all three jurisdictions studied. In the United States, a handful of states, although recognizing smart contracts within their commercial code

within the private domains, have not exploded the potential applicability of smart contracts to public contracting (Zamani et al., 2018; Liu, 2021). For civil law countries, awakening smart contracts with deep- seated administrative discretion deeply rooted within public law places more burdens on lawyers researching smart contracts. Given the objective, this research intends to develop frameworks for procedural fairness, reversibility clauses and judicial review applicable to the smart contract ecosystems found in public tenders.

3. How can privacy-preserving technologies be successfully implemented to reconcile immutable data on a blockchain with data protection obligations under the GDPR and North American privacy laws?

The current literature suggests the possibilities of off-chain storage, selective disclosure, and cryptographic blurring of PII as remedial actions (Bernabe et al., 2019; Akanfe et al., 2024) but have not undergone demonstrative testing in legally binding government environments. Additionally, Canada's federal and provincial data privacy regimes and the U.S.'s sectoral data privacy regimes create complex and different compliance scenarios. One area of research could include the technical–legal translation of privacy technologies to practice, with the requirement of valid attribution to formal evaluation metrics and legal opinions.

4. What mechanisms can be utilized to assessing and minimize the environmental and monetary implications of implementing blockchain in public procurement systems?

It is important to acknowledge the continued demand for climate-conscious public technologies publicly funded in jurisdictions like Canada and the European Union; and to be aware of the energy and scalability tradeoffs of blockchain (Min, 2019; Upadhyay, 2020). This question advances towards the development of life-cycle assessment models addressing the adoption of blockchain technology based on not only technical feasibility, but also carbon intensity, monetary cost, and alignment with green digital public policy objectives.

5. What governance frameworks and procurement standards can be used to mitigate the risk of technical lock-in and promote flexibility in public blockchain systems?

As the risk of vendor lock-in and transparency risks increase with the technical complexity of blockchain system design (Tan, 2023; Sanka et al., 2021), particularly in long-term government contracts, future research should prioritize modular design, open standards, and participatory governance models. In a federal system like Canada, or in the decentralized procurement landscape, such as the United States, creating blockchain platform designs that provide for flexibility but also responsibility and accountability involves compromises between technical interoperability and legal pluralism along with administrative diversity.

These questions would map the multi-faceted nature of blockchain risks and reveal the value of ontological and interdisciplinary inquiry in this area of study. Each question also speaks to a larger tension seen within digital governance, such as using new technologies to bolster or create value while at the same time undermining legal certainty, equitable administration, and environmental

responsibility. For the purposes of this dissertation, these questions will provide a foundation for both the theoretical framework and methodological design in the subsequent chapters related to the ways in which Italy, Canada, and the U.S. have confronted these issues during the modernization of their procurement approaches.

The risks and challenges of blockchain implementation in the public sector—underscored by the realm of public procurement—should be understood not solely as operational hurdles, but as structural and normative tensions that intersect with the goals of transparency, accountability, and anti-corruption. The risk categories explored in this subsection illustrated that blockchain is not an all-purpose enabler, but exists in—and is limited by—situated legal architectures, institutional logics, and political contingencies. Therefore, the potential of blockchain to improve procurement integrity in Italy, Canada, and United States, must also be viewed against these intractable challenges.

From an anti-corruption lens, blockchain's attributes of immutable audit trails and tamper-resistant registries strongly rhymed with previous calls for more transparent procurement ecosystems. But the literature highlighted the possible downsides of blockchain—despite its immutable audit trails, it must still be constructed into an institutional, legal, and regulatory context. The inability to reverse bad transactions, amend bad or unwanted smart contracts, and conform with requirements for data erasure provides new forms of inflexibility that are different from standard legal and due process protections located in governing statutes—essential features of accountable governance (Shermin, 2017; Sousa, 2023). In other words, blockchain's technical integrity is not synonymous with legal and ethical legitimacy.

Furthermore, while it is concerning that repeated examples of technical centralization (i.e. through validator collusion, unwanted ownership from vendors, or obscure governance processes) are problematic by themselves, the implications in anti-corruption situations are more troubling. When a monopolistic set of actors control the infrastructures on public procurement platforms, these actors may only continue, or likely strengthen, non-transparent practices, in part due to the lack of independence in system design or operational capacities (Esposito et al., 2025; Dziundziuk & Dziundziuk, 2022). This indicates that unless governance mechanisms are truly democratized and institutional accountability is instituted, blockchain may operate as a preserving mechanism of power asymmetries in public procurement instead of a disruption mechanism.

In jurisdictions where there is little to no digital sovereignty, or capacity to innovate approaches to procurement (i.e. experimenting), lock-in potential may be a serious issue. Governments that use proprietary blockchain systems with no modular components or exit strategies may result in future hurdles as they try to comply with new legal requirements, adopt new technologies, or respond to public accountability (Malik et al., 2021; Tan, 2023).These themes carry particular relevance in Italy, where a centralized system blocks pathways for flexibility while also ramping up the potential for irreversibility of technology, and the U.S. where current federalism limits cooperative governance requirements to standardize any upgrades.

Therefore, while the possibilities for blockchain to support procurement transparency are clearly identified, the risks that it poses (if allowed to exist) may, in turn, negate the positives that blockchain offers. The literature certainly identifies that careful governance choice, legal-technical alignment and institutional capacity development are prerequisites to any sustainable anti-corruption benefits. These factors would undoubtedly become important considerations in subsequent chapters of this dissertation which will consider how Italy, Canada, and the United States address these factors, and in turn, whether they make any progress on procurement disclosure.

In summary, implementation of blockchain in public sector contexts - and for purposes of this dissertation principally in procurement processes - produces a multifaceted risk landscape which calls into question the theoretical assumptions of neutrality and inevitability in technology. As I have shown through critical engagement with the academic literature, the benefits of blockchain, like immutability, automation, and decentralization, are dependent upon choices of design, and when it comes to the law, legal context, and institutional capacity. The five core risk domains examined in this subsection - technical centralization, immutability of smart contracts, jurisdictional tension (data privacy), energy and scalability, and governance lock-in - are not distinct issues, but bundled risks that arise together on how blockchain might contribute to more or less public accountability.

Based on the scholarly discourse, while technical capacity may improve transactional transparency, it cannot exist outside of the governance system that will utilize it. And that governance system must allow for feedback loops, legal pluralism, administrative discretion, and sustainability parameters to be adhered to. If not, blockchain solutions will be technocratic, exclusionary or opaque, like any other technology, and particularly when such technology is intentionally deployed in legal systems that hinge on an exercise of due process, proportionality, and regulatory responsiveness. If these unintended consequences were not anticipated, the outcomes could exasperate implementation costs, erode public trust, or allow opportunistic forms of institutional capture to masquerade as digital change.

For your comparative reflection on Italy, Canada, and the United States, these analysis outcomes can provide impeccable analytical depth. Each jurisdiction will not have the same risks, but different perceived configurations of the risks as they may be affected by their own procurement systems, forms of legal doctrine, and digital policy environments. For example, each country will have its own challenges: Italy faces some legal friction with centralized procurement and GDPR obligations, Canada has its own interoperability issues related to federality in its digital governance, and the regulatory ambiguity institutionalized in the U.S. produces fragmented compliance across all states; all of which form contextual nuances that require forms of risk mitigation, much of which finds itself theoretically underdeveloped or untested in existing literature.

The gaps and unresolved issues identified in this subsection, will ultimately inform the bridge to the next stage of this literature review: an assessment of the potential for blockchain to contribute to anti-corruption and institutional reform in public procurement. While Section 2.2.2 has assessed some of the barriers to the implementation of blockchain, the next subsection will provide a critical assessment of how despite the aforementioned risks, blockchain may hold regulatory potential for transformative action, provided that alignment, foresight, and participation are priority criteria at each phase of reform.

Discussions surrounding blockchain adoption in public sectors, including procurement, have typically assessed the technical and operational dimensions of the technology, including scalability, interoperability, energy use, and rigidity of smart contracts. These facets are particularly relevant, but often the ramifications of those issues are not examined, relative to socio-political pushback to change and to the divergence in levels of institutional preparedness—two variables which could result in decidedly different outcomes of adoption irrespective of the technical complications. Scalability, for example, is often evaluated in a purely technical manner, measured by transaction throughput, and latency, while evaluated in the public procurement arena, may be even less about the technical constraints and more about the potential limitations of institutional scalability—i.e., whether the agency has the administrative bandwidth, the requisite human capital, and governance process, in which to utilize a blockchain system—or whether bureaucratic structures lack the agility to even process new workflows; or if it recruited procurement officers with experience in managing digital contracts.

Interoperability challenges do not escape the intrusion of political dimensions either. In technical terms some of the overlap is established if a blockchain application can integrate with a legacy procurement system through the use of standardized data formats, (with) API endpoints, and without layering more cyber security frameworks on top of existing ones. Yet in many jurisdictions today, the 'old' system(s), by way of example, might not just be out of date - they are politically or socially entrenched. Legacy platforms, supported by vendors who employ politically expedient relations to protect their existing proprietary architecture, create a sense of political economy agency, and are often viewed as a material construct of influence networks that stand in opposition to the adoption of blockchain technologies. This is precisely aligned with the research gap that exists in regard to level of actor or individual resistance, where individuals could still be opposed to the adoption of blockchain technology for reasons that are more about networked power relationships than about doubt generated from a lack of certainty about the use of procurement.

The rigidity of smart contracts produces both legal and institutional hurdles. As automated contracts minimize the sincere opportunity for discretionary interference, the lack of flexibility for a procurement officer to pursue procedural opportunities for exception to be made under procurement law, such as during an emergency procurement involving specifications in the national interest, creates a tension while lacking continency governance spatial updates. Without adequate governance contingency frameworks, rigid automation will protect certain means for methodology variations that create a complacent space for lack of trade-offs that would promote

willingness for institutional adoption. These tensions indicate there is a need for a legal-technical co-design processes that build the necessary legal-space for code-based systems for a given enabling legislation in respect of the relevant statutory requirements for procurement, a practice relatively absent in the prescribed literature.

The objections to energy use—particularly if consuming energy on a public or permissionless blockchain—are often examined through dimensions of environmental or cost into the issue, while can be dictated by political prioritization for adapt penetrative change. For instance, in the case of EU members, such as Italy, introducing protocols with high-energy profiles might be politically considered unacceptable, regardless of the technical merit—the impact of which could imply one more obstacle in the path to adoption. This consideration brings forward the very important significance of 'policy narratives and public perceptions' that make up institutional readiness, that are typically missing from technical evaluations of blockchains energy considerations.

The research literature also underestimates how the governance characteristics of blockchain and distributive ledger systems may affect institutional adoption. To give a couple of examples, the selection of validators in permissioned consortia can easily become a location for political contestation. For instance, if members of a consortia have concerns about the potential for collusive behaviour among validators, the stated trust between members and their use of the platform can be undermined in the minds of each member if the governance procedures to manage validator selection process and mechanisms for dispute resolution are less than transparent. Furthermore, governance models which democratically incorporate an approved process for establishing and managing users' access to blockchain inputs and outputs introduce their own significant transaction costs which may infuse exactly the types of opacity which block chain was engineered to eliminate.

With those interdependencies in mind, I highlight that, for this dissertation, I do not consider these interdependencies to be peripheral to an understanding of the reasons why institutional adoption of blockchain-based systems to public procurement often stall. My study integrates a technical assessment of blockchain with a broader institutional or political economy analysis which has significant potential to address the gap in economic assessments of blockchain due to incorporating realistic context-specific factors into assessment of blockchain’s business model for anti-corruption.

With respect to existing studies in the scholarly literature on applying blockchain technology to the public sector which are primarily focused on procurement, the most frequently-identified operational and technical risks are typically referred to as scaling, interoperability, smart contract rigidity, and energy consumption. While these studies may touch on issues related to risk or constraints on scaling or interoperability as integration problems with data standards, APIs, or cyber security protocols, they neglect entirely how blockchain’s interoperable or scalable risks are impacted by socio-political resistance, and the different stages of institutions’ readiness to adopt blockchain-based systems. The explicit or implicit omission of external socio-political resistance

factors, along with various states of institutional readiness to adopt blockchain systems, detracts from the explanatory utility of independent studies and is also linked to a significant gap in scholarship which I have identified in my research.

In practice, ecosystem scalability is generally understood as computational throughput, latency, or consensus efficiency. In public procurement contexts, more emphasis should be placed on institutional scalability, which refers to the capacity of agencies to adapt workflows, retrain human capital, and align or separate levels of multi-level governance structures. Often times before we consider public procurement platforms system performance, institutional scalability may be the more binding constraint than system performance. More to the point, a technically-sound platform will struggle to provide the same resiliency if public procurement offices lack digital literacy, or if entrenched bureaucratic hierarchies are philosophically opposed to decentralizing elements of their control over procurement, or if there are inadequate inter-agency distributive mechanisms. The literature thus critically omits the discussion and consideration of the internal and external readiness factors, which results in overly optimistic predictions of the deployability and sustainability of a blockchain-based system.

Interoperability, faces similar shortcomings. The challenges of interoperability are typically framed solely in technical terms of integrating blockchain networks with legacy systems relative to data standards, API connectivity, and cyber security protocols. In practice, interoperability simultaneously must also deal with political or economic factors associated with legacy procurement systems, because legacy procurement systems are often controlled by entrenched vendors, who will benefit from contractual and political leverage to strike against new open/blockchain-based approaches. This economic resistance is not necessarily passive; in some cases, vendors will lobby actively against transitioning to newer and open transparent systems, especially when the system will undermine their own revenue sources and discretionary spheres of influence.

A third frequently-cited risk, smart contract rigidity is generally presented as a technical limitation that cannot accommodate exceptional procurement scenarios. In contrast, smart contract rigidity, when viewed from an institutional lens, may provoke pushback from institutional players like agencies' legal departments, or other procurement units with valid fixity for exercising discretion in certain situations (for example, a legitimate emergency contracting scenario, or a very legitimate national security complaint). If the new blockchain-based system is the first project within the governance framework of the agency, and there aren’t sufficient or meaningful governance mechanisms to allow for the flexibility that contract rigidity requires, any internal push-back on expedience due to the variables of legal non-compliance, or non-compliance to their selected operational strategies around procurement may stall its internal operationalization process.

Concerns about energy consumption for public, permissionless blockchains are commonly framed through either environmental or cost lenses. In political contexts which prioritize sustainability distinctly (for instance, the European Green Deal), as the energy intensity of the blockchain

increases so too can its capacity to highlight opposition from environmental NGOs, budget committees, and environmental watchdog agencies. In these cases, energy efficiency is translated from a design consideration to a political prerequisite for institutional approval and funding.

Although no transformation involving technical and operational risks can be credibly considered and assessed in isolation from socio-political resistance, opposition, or institutional capacity. This dissertation invites the gap in feasibility assessment literature by embedding a political-economy lens into feasibility assessment. Specifically, the dissertation will test how institutional structures, stakeholder incentives, and administrative cultures affect the translation of technical design leverage into operational transformations. By focusing on these dimensions, this study aims to move beyond the narrower assessments of technical feasibility, which limit their capacity to provide a realistic evaluation of blockchain's potential to contribute to anti-corruption efforts in public procurement.

2.3 Blockchain for Governance and Anti-Corruption

Increasingly, blockchain technology is being viewed as a systemic approach to problems of transparency, accountability and integrity in the public domain. The crucial debate is the propect that the technical characteristics of blockchain - immutability, decentralized consensus, traceability, and automation - will reduce discretion and provide the capacity for all actors in the public domain to verify the public process in real time. These characteristics align especially with anti-corruption goals in the public domain, where decisions are rarely made transparently, actions are difficult or impossible to audit, and corruption can occur quietly and often invisibly. The literature we explored, demonstrates how blockchain systems, integrated into procurement, auditing and legal documents workflows can be used not merely in a technical sense, but as an innovation in governance.

Bruschi et al. (2022) conducted a system for on-chain tenders that run on the Ethereum blockchain, which is a novel addition of their study..The authors outlined the comprehensive procurement processes, including tender issuing, bidder registration, bid submission from the registered bidders, bid evaluation, and the announcement of the winner using smart contracts. The authors are concerned with the risks involved with a tendering process, and they have built a protocol that makes it impossible for anyone other than the smart contract code to modify each stage of the procurement process. Because each step is cryptographically recorded and verifiable by the public on a blockchain, the protocol provides a tamper-proof, auditable pathway that minimizes the opportunities for bias or manipulation after the fact. Moreover, it offers a framework that allows third party observation because all steps (tender process) in the procurement process can be validated ex post. Therefore, the authors successfully demonstrated that blockchain had the potential to mitigate corruption, without requiring a complete transformation of institutions, at all points of the procurement process.

Furthering this viewpoint, Latha and Chinnaiyan (2021) proposed a Blockchain-as-a-Service (BaaS) model for public e-tender management with smart contracts that govern both the tender

submission process and the quality assurance and compliance verification. By bringing together all relevant actors in a multi-stakeholder shared blockchain ecosystem including the state authority, contractors, and independent auditors, the BaaS model sought to create levels of trust and consistency. The authors also acknowledged the following challenges: confidentiality of data that can be obtained on public blockchain, scalability for hundreds of millions of tenders each year, and the necessity of creating new legal precedents to acknowledge the veracity of contract agreements stored on blockchain. Their contribution reinforces that blockchain's utility for anti-corruption is best realized not in isolation, but with institutional, legal, and organizational change.

Agwot (2024) explores systemic and behavioural factors influencing corruption in public procurement, articulating valuable context for Blockchain's role within anti-corruption structures. Agwot compares evidence across multiple jurisdictions to uncover asymmetries of accountability, opaqueness of information, and discretionary power (subjective). They suggest improving the capacity of institutional readiness, the existing and digital audit firm capacities, capacity to issue a report from the record, is an important foundational condition to reduce corrupt acts. By exposing these structural vulnerabilities, Agwot establishes the complementary nature of technical affordances offered by Blockchain immutability as an audit tool and the distributed oversight it can deploy, with the systemic considerations that must occur to institutionalise integrity in public procurement. (Agwot, 2024)

Alotaibi (2023) proposed a conceptual model of continuous (embedded) government auditing using blockchain technology-based smart contracts. Alotaibi proposes to validate automatically every government interaction or transaction, potentially every stage of a procurement process, in response to pre-defined rules coded into the social smart contract. After the transaction, the distributed ledger with the audit trail provides a permanent record available for internal and external auditors to explore. Alotaibi describes a system that offers to change the framework of auditing; to move from retrospective and periodic to ongoing and real-time oversight, reducing the potential for deliberate bad acts over time and increasing accountability to the immediacy of the act. This integration into institutional context is not just governance as a way to design - a change from thinking of auditing at the end of process (Alotaibi, 2023).

Anyanwu et al. (2023) examine the use of blockchain technology in different use cases across the different levels of government across the United States within a national narrative beginning with their national-level review and describing about blockchain's impacts on efficient, transparency and corruption management controls. In the review the authors illustrated that the blockchain pilots on identity management; land registries; and procurement systems improved measures of data integrity and errors fairly well. However, the authors noticed some challenges emerged in scale; integration; jurisdiction or regulatory concerns. The authors recommended for adoption to be sustainable, agencies not only had to be technology-ready, but also partner or coordinate across agencies to encourage training and policies, and reiterated the blockchain-anti corruption interface needs to be established, backed-up by strong governance structures. (Anyanwu et al., 2023).

Alves Batista (2024) approached blockchain as an effective means to deter records fraud in the public procurement in Brazil using a qualitative case study designed to discounted a couple of pilot studies. In the study, Alves Batista presented some main issues amongst the public agency respondents regarding a tamper-evident audit log that would rapidly and definitively identify those predated contract changes, due to blockchain implementing specific risk mitigation in the public procurement cadre. The author also noted an increased level of trust amongst stakeholders, all of which were aware of tender and award documents that the public contracts created newly visible. Still Also noted implementation tensions such as data privacy concerns; regulatory issues; but made the salient point that for technical transparency to be transformative in improving anti-corruption strategy, policy infrastructure is really needed. Alves Batista has made a significant piece of work, as the study is grounded in strong technical treatment, combined with empirical validation as public procurement oversight reforms are both feasible and achievable through blockchain technology. (Alves Batista, 2024)

Bennett (2024) concentrates on the amplified potentials of blockchain technology in terms of transparency and traceability because they are focusing their search on the procurement system for Italy's chains, as the potential focal points to their inquiry. By collaborating these perspectives through identified in their analysis which emphasized the oversight of the complete system, through chain of custody areas - looking across the spectrum of the supply chains. Bennett's case study illustrates the possible elimination of colluded behaviors amongst suppliers that resulted in unjust invoice pricing and possibly supported better chain of custody. Bennett's case study should expand these supply chain considerations to include the characteristics of transaction events, particularly regarding all levels of procurement workflows where contractors may subcontract a task concealed to multiple sourcing levels as activities remain equally obscured for both final delivery and payment throughout the transactions. There are clear possibilities for the characterizing unequivocal, traceability potential through blockchain as an obvious deterrent for any corruption tendencies across any record-keeping procurements. (Bennett, 2024)

Bouaicha et al. (2024), offered review a public procurement type solution for integration or learning offered a specific blockchain for Italian public procurements style, to include its anomaly exclusion, concerning identifying and signaling the distinct irregular bidding behaviors. As a pilot project, the students offered a unique permissioned block-chained environment , that would apply a machine learning classifier to signal not only the different stages; but also revealed any suspicious activities from each of the stages; with an overall outcome analysis of the undue relationships across the different stages of public procurement tender project and delivered it in real time instead of waiting for human acceptance behaviors patterns to occur (as the tender would just appear suspicious so a part of the submitted submittal, so all could be found immediately). Work offered some quantifiable amount of controlled integrity and stakeholder trust, some level of a reduction of all behaviors exhibited in the pilot project. Complex corruption vectors significant tensions as a need to partner the technically reliable blockchain innovations with fact-based

governance, as well as some possibly solid measures to identify anomalous behaviors with less human circumstances. (Bouaicha et al., 2024)

Cagigas et al. (2023) have developed an evaluative framework for blockchain use in government contexts, linking digital attributes to governance goals (e.g. transparency, efficiency, citizen trust). The authors base their framework on systems theory and highlight a number of examples from various national contexts. They conclude that the anti-corruption potential of blockchain systems is dependent upon a variety of factors linked to institutional maturity, digital policy ecologies, and regulatory tensions. Relevance to public procurement was emphasized when they note that the success of pilot projects should be contingent on the end-to-end integration of the procurement process from announcing the tender, to selected bidders, to managing the contract, to auditing it. This model provides a diagnostic view of blockchain readiness from the procurement ecosystem.

Čeke, Buzadija, and Kunosić (2022) researched a potential enhancement to the procurement process utilizing smart contracts, which was piloted at a local government. By automating important milestones in procurement, including bid submission, evaluation criteria, and decisions to award contracts, they effectively eliminate options for vendors to modify their bid post-bid award selection and options for ad hoc vendor re-evaluations post-award. Reporting that concerns related to decision-making opacity were remedied and procedural consistency improved across a range of characteristics they also found that areas for improvement included UX and inter-system integration. This study helps to substantiate the broader narrative that smart contracts can be built into the operationalization of anti-corruption principles in public procurement practice.

Diadia, Tamgno, and Kora (2022) developed a "dematerialized" procurement model developed using Hyperledger Fabric compliant with the Open Contracting Data Standard (OCDS). This architecture integrated blockchain with "standardized procurement metadata," allowing them to ensure transparency of bids and open data compliance through their new system. Data integrity was improved through incremental ledger entries that can never be changed, while obsessive compliance with the OCDS allowed users to get data that could be directly compared and reused across jurisdictions. As such, for better technical alignment with the defined standards in e-procurement. The authors strongly imply that technical alignment with e-procurement standards greatly enhanced blockchain's unique capacity to reveal and avoid corrupt manipulations in the preparation (and evaluation) of tenders.

Doguchaeva, Zubkova and Katrashova, (2022) research the blockchain applications for public supply chain management as it relates to procurement fraud and risk management. The study examines blockchain's major strengths in securing transactional data and providing full trace visibility from the issuance of a contract to the delivery of goods. The authors warn enumerating and tokenizing real-world assets and leveraging physical verification systems remain important to decrease risk for common misses of “oracle” failures" and misrepresented reality as fraudulent representations of reality. Their research highlights that data integration and operational controls

are paramount to the success of blockchain in procurement situations such as the above (Doguchaeva et al., 2022).

Dubey, 55) typing a three- phase pilot using a blockchain enabled tender allocation model included game-theoretic bidding and reputation scoring in a simulated procurement context. Half of the participants used smart contracts to automatically short list bidders based on predetermined quality-price criteria interpreted with their prior bidding behavior. In addition, performance and compliance rules, proposals using smart contracts embedded were stored in the blockchain when submitting both after the third phase of tenders and utilized results of each bids terminology through effective bid request metrics. The authors highlighted that although the bidder's subjectivity may still persist, the system is virtually impossible to manipulate after a tender award. Successful bidders will find themselves subjected to any previous performance compliance rules both during and after the awarded contract. The writers completed the paper citing technical integration with completely objective systems and are excited for the opportunity that buy and stand-alone bidding can present through algorithmic neutrality. They posed a challenge that scale and legacy systems and the many opportunities for their model to improve procurement through integrity (Dubey et al., 2023) too may be lost.

Dziundziuzk and Dziundziuk (2022) undertake two complementary studies of Blockchain's anti-corruption potential for public administration reforms. The first study explores the current governance-related decision-making choices, while the second studies the use of platforms to advance and modernize administration for an organization. Both examples describe a beneficial and iterative design of blockchain into public authority and decision-making workflows not limited to license approvals, report approvals, budgets, or supply chain decisions without discretion associated with the decision. The authors referred to the importance of organizational readiness and stakeholder training and legal frameworks as preconditions to unlock potential anti-corruption in any manner mentioned in the two parts (Dziundziuk & Dziundziuk, 2022a; 2022b).

Fonderico, (2024) considers the Italian environment and explores how the reformed Italian Public Procurement Code incorporated statutory anti-corruption measures. While legislation predates the widespread use of Blockchain the authors identify and determine visible paths of opportunities at the intersection reform and technology enforcement mechanism ---Blockchains. Fonderico, (2024) argued through potential code and evidence-based accountability recordkeeping in the anti-corruption element of the code, compliance monitoring and forensic audits by an immutable ledger, may further the reforms from the code and any technology development with innovation in full.

The work of Sánchez García (2019) examines an example of how mandated planning (programmazione) in Italy's procurement regime may be used as a lever to facilitate upfront transparency before a contract's tender, presenting the argument that Plans, specifications and evaluation criteria made public early in the process will limit the ability to change, manipulate or intentionally create ambiguity downstream. This line of reasoning has elements of a ledger design

that would use time-stamped plans and specifications and evidence of alteration as a substitute for institutional information that would ideally not be available for re-adjudication.

Gola et al. (2023) present a Bank of Italy Occasional Paper which maps governance options for a distributed-ledger system across permissioned and permissionless design considerations, stressing considerations around access control, rules and degrees of representation as determinants of resilience and fit to the existing institution. Their governance taxonomy is useful in the context of setting pertaining to complex multi-level procurement, where there is a dilemma about the need to co-design the tech architecture with administrative governance responsibilities.

Mezquita (2021) provided an early draft of an exploration of blockchain-enabled tendering workflows, however the work was promptly retracted so is only a matter of ongoing historical interest around the proposed routes for technical approaches to the topic and shouldn't be treated as probative for feasibility or estimated impacts.

Gong et al. (2021), by contrast, present an implementable e-tendering framework on Hyperledger Fabric, which automates the bid submission, scoring and validation process through smart contracts as well as automate traceability actions and reduce reliance on centralized intermediaries—an example of what occurs when procurement rules are abstracted and incorporated into executable logic rather than relying solely on institutional trust.

Finally, Telles (2022) provides a rich synthesis of lived spills and deploys, noting that the projects in Aragón (Spain) and Colombia were paused at the pilot stage, but the project in Peru advanced to production—a reminder that institutional compatibility, clear regulatory mandates, and stakeholder trust all contribute to whether what was once a technically plausible pilot develops into a functioning system.

In combination, these sources support a cautious thesis perspective: the potential for blockchain to act as an anti-corruption capability in public sector procurement depends (much less on the technically plausible coded capabilities) upon the relationships between the governance choices, the legal transparency obligations, and the administrative routines that we expect to shape the technical capabilities into lasting change.

Gong et al. (2021) demonstrate an e-tendering evaluation framework on Hyperledger Fabric that automates the bid submission, scoring, and validation processes, while maximizing traceability. Their prototype strengthens the contention that blockchain technology can maintain the integrity of the scoring pipeline if it is to be integrated with the bid process, and the smart-contract layer itself can interface clearly with existing procurement platforms and data structures (Gong et al., 2021).

From a design-operations standpoint, Haffar & Özceylan (2024) illustrate how smart contracts may be utilized to implement multi-criteria supplier selection that integrates considerations for quality, sustainability, and previous supplier experience. The supplier selection process is of great concern, as it is a contact point that is often associated with personal biases (discretionary) and gone "rogue" toward corrupt practices (collusion) on the part of the procurer. Haffar & Özceylan (2024) also demonstrate how the scoring logic must be auditable, and how on-chain auditability might provide assurance to the public and identify relevant sustainability commitments.

From a macro-level perspective, Ibrahimy, Norta, and Normak's (2024) systematic review of the application of blockchain's governance models across public services synthesizes several success factors (interoperability, legal clarity, and stakeholder engagement, to name a few) to assert that gains in anti-corruption can only be achieved once technical infrastructure is nested within supportive institutional arrangements (Ibrahimy et al., 2024). In concert with this, Kálmán (2024) described the fragmentation of regulation globally as a "mosaic" and pointed to the tension between immutability and data-protection rights (e.g., erasure), and concluded that responsible and durable deployment could only occur if the platform is co-designed alongside the administrative law (and privacy law) framework (Kálmán, 2024).

Taken as a whole, these sources back the modest claim that blockchain's potential to support anti-corruption in public procurement is predicated less on the technical capacity of x, and is instead a function of governance choices, duties around legal transparency, and administrative practices that convert provider capabilities into utilitarian, enforceable, and auditable changes.

By methodically identifying the legal and regulatory covers over blockchain in a comprehensive sample of countries, Karisma and Tehrani (2022) complement this perspective. They categorize regulatory responses as either "enabling" and "prohibitive," and include that enabling legislation supports blockchain pilots in the public sector, particularly in cases of procurement and administrative transparency initiatives. However, they state that success depends on described heinousness regulatory certainty regarding digital signatures, smart contract enforceability and liability of data. Their discussion found that without politically capitalized targeted enabling regulations, blockchain's promise to support improved governance and decreased corruption will remain largely aspirational. Lebron & Lamoreaux (2017)

Mustafa et al. (2025) connect legal, technical, and ethical perspectives by presenting a blockchain-governance model for e-government. The interdisciplinary model describes its necessity that smart contracts must be supported by a legal contract and incorporated with an ethical audit process to mitigate risk. The issue of anti-corruption is convincingly framed into digital governance design, embedding features like auditability and non-repudiation in governance design enables fully compliant and trustworthy e-government (Mustafa et al., 2025). The authors reinforce that technology architectures need to be aligned with legal systems in order to replace the discretion of bureaucratic actors (Mustafa et al., 2025).

Ochigbo et al. (2024) use a governance framework that draws on wider regulatory frameworks for digital transactions across national jurisdictions to consider blockchain-based systems. They note that countries with integrated regulatory frameworks in areas such as digital identity, contract law, and standards for data have created the conditions needed for pilots with blockchain, such as asset registries and procurement. In contrast fragmented legal regimes are seen as a source of uncertainty delaying adoption of the technology and its anti-corruption power to mitigate risks. The authors suggest that legislative cohesion and design integration across the various public service sectors will be needed in order to translate blockchain's technical potential into governance solutions (Ochigbo et al., 2024).

Mazloum, Abdelkader, and Mazloum (2022) express empirical evidence from the pilot operations of blockchain based systems as Smart Institutions. Their study examines how recording transactions in real time in an auditable ledger as part of an operational workflow in government allows to impose auditability and limit the space where discretionary abuse could occur.They illustrate the role of immutable processes as a method for reaffirmation of internal integrity and institutional responsibility—in particular procurement transactions—by distinguishing an unverifiable paper process from a nurturing cryptography-based record. The authors suggest that at least partially, such veracity can be engendered by assurance of staff training, and governance support (Mazloum et al. 2022).

Mazloum's work connects directly to Piccardo, Conti, & Martino (2024), that synthesizes nascent blockchain instantiations across public services. Their survey identified procurement as an important sector not only for securing tender documents, but also for smart contracts, and enabling records access for citizens. They classified use cases—something like identity, supply chain, tendering, as a means for examining blockchain as a horizontal infrastructure for anti-corruption to underscore the multi-sectoral governance system. They ultimately found that although challenges exist such as cost of adoption and legal uncertainty, blockchain appears to be a valid means of incident integrity (Piccardo et al., 2024).

Pokharel & Kshetri (2024)'s case defined a possible hybrid program called "BlockLaw" which could include blockchain technology applied to legal transactions potentially coupled with automated legal workflows, and cybernetics modules. This form of theory suggests that if you were to fold legal regulations into smart contracts that dictate technology driven enforceability such as transparency requirements, and penalty clauses, you could align ethical governance into known technological enforceability. This theory model would help facilitate knowledge transfer between the gap in cooperation between blockchain code, legal texts, and agent compliance frameworks – an entirely new pathway to possibility to resolving a historically slow administrative process under a rule-based view of governance, and potentially deterring corruption in advance. The multi-layered nature of the enactments (legal + technical), contributed to a greater understanding of blockchain capabilities highlights the transformative potential for systemic governance—not just documentation (Pokharel & Kshetri, 2024).

Radonjić, Bojić, & Novaković (2024) provided an important review of blockchain development, and challenges to realization, and the potential governance consequences of blockchain implementation within the public sector environment. In their cross-national case recommendations, they provided barriers such as economic, legal, and institutional inertia as key blockades to movement. They argued that blockchain could enhance transparency in procurement, and restore public confidence in public services in developed jurisdictions, but only with sufficient public investment, economic viability, and related regulatory collaboration. Their observations warned that any exploratory or pilot case experiments tend to reflect the degree of local governance maturity that is more so about a willingness to figure out governance framework implementation by informed design than by technology design (Radonjić et al., 2024).

Ramya et al. (2024) introduce the "Block tender" procurement platform a trustworthy purchasing application featuring reputation-based bidding and smart contract compliance checks. Initial pilot simulations feature reduced access for supplier collusion and post-award renegotiation. Block tender's overall design intends to maximize end-to-end transparency and places blockchain firmly in the governance-by-design paradigm, obviating corruption through automated rules and verifiable contract performance (Ramya et al., 2024).

Trequattrini et al. (2024) conduct a systematic literature review, establishing that blockchain supports anti-corruption by establishing immutability, auditability, and decentralized verification mechanisms for a public system. The meta-analysis further established procurement as an area of substantial research, and emerging evidence suggests associated tamper-proof ledgers and smart contract systems diminish both the incentive and opportunity for corruption by minimizing the discretion of administrators (Trequattrini et al., 2024).

Wadegaonkar et al. (2024) describe a smart procurement and contract management solution utilizing blockchain. The solution was tested in pilot projects leading to procurement solutions and contract management systems within municipal administrations. Their implementation automates the release of payments upon milestone verification using smart contracts, thus minimizing human interference and aligning public funds, with flow barriers defined on-chain. The pilot project experienced faster processing times, improved audit transparency, and reinforced in the real-world urban governance environment that blockchain can implement anti-corrupt controls (Wadegaonkar et al., 2024).

Wamba et al. (2024) examine blockchain-oriented public sector projects to assess the prospects to address prominent organizational risks. Their findings establish that projects with blockchain—including procurement platforms—showed improved process integrity, and reduced leakages. Importance was placed on the benefits of governance maturity, and stakeholder engagement, thus reinforcing the argument that blockchain must be discussed as a technology in an adaptive

institutional ecosystem (Wamba et al., 2024). Wibowo and Yazid (2023) offer a systematic review of barriers and enablers for blockchain adoption in governmental contexts. They categorize the barriers to blockchain adoption involving government actors into three main categories - use of digital technology (broad technical barriers), the skills gap for its implementation, and organizational barriers - but they then encourage exploring procurement applications as examples of high maturity use cases, where the indications for standardization of process, and, the ability to meaningfully demonstrate transparency of the contract are features that can greatly benefit from immutable properties of blockchain technology. In other words, they may emphasize that the technology is best utilized for use cases adjacent to anti-corruption, especially when the workflows are structure by clear procedure (Wibowo and Yazid, 2023).

The literature outlined above offers enough rigor to suggest that blockchain technology presents opportunities for increased transparency, accountability and integrity within public procurement systems. The 48 reviewed studies in this body of research indicate a cohesive view of the technical traits of blockchain technology - such as immutability, decentralized recordkeeping, real time audit ability, and programmability/impossibility of contracts through smart contracts - as mechanisms aimed directly at the very structural context within which corruption often develops. Yet, upon deeper analytical reading of these studies, and despite these conceptual and experimental confirmations, there are significant limitations present in the literature in the context of this dissertation's interest in comparison, regulation and mechanisms.,

The literature suffers fundamentally from jurisdictional silos. While there are mentions of Italy (Bouaicha et...., 2024; Alves Batista, 2024), Brazil (Mazloum et al., 2022), and some examples from the United States (Anyanwu et al..., 2023), there are no really acute bindings in the cross-comparative documentation to suggest that extensive research was developed on the same subject.

The significance of diverse legal families, as highlighted by the contrast between civil law in Italy and common law in Canada and the US, is almost wholly ignored. Comparative claims arise in parts such as Telles (2022) and Wibowo and Yazid (2023), yet remain abstract or descriptive. The chief identified void in this dissertation confirms, despite varying legislation, case law, and regulations, there are no contextual, legally sensitive analyses that show how blockchain adoption is impacted by not only its technical possibilities, but also distinctly different constitutional, regulatory, and administrative systems. The gap this dissertation explicitly seeks to populate using a tri-jurisdictional legal comparison method.

Notably, the literature often emphasizes enabling or constraining environments, but it also conflates law and regulation and often views "governance" as a singular element. A small number of contributions distinguish legal codification from regulatory experimentation—mostly sandbox programs or pilot exemptions— Kalman (2024), Mustafa et al. (2025), and Karisma and Tehrani (2022). Even in these cases, the contributions are descriptive or still not analytical because they dont demonstrate or explain how law, administrative regulation, and policy instruments dynamically interact to shape trajectories of implementation. In contrast, this dissertation's tri-

dimension of legal framework, regulatory approach, and technological affordance distinguishes three important parts of this dynamic process allowing a more faceted tool for understanding how blockchain may embed legally and legitimizing institutionally in different procurement ecosystems.

Importantly, the literature presents significant functional abstraction. A multitude of papers (many) like Trequattrini et al. (2024) and Wamba et al. (2024) extol blockchain as a generic transparency-enhancing mechanism, but few, if any, detail how quantitatively specified transparency-enhancing functionalities match up with specific corruption risks. Mechanism-risk fit, for example, how timestamped bidding logs might counter bid-rigging or how smart contracts might neutralize ad hoc contract renegotiation, has not been examined. This limits the practical contribution posed by otherwise fruitful results. A major contribution of this dissertation is the presentation of a corruption-specific typology that matched up with blockchain functionalities presented alongside an articulation of procurement corruption vulnerabilities. This facilitates a more substantive match between technological mechanisms and their adoption around procurement vulnerabilities, and moves the conversation from hypothetical to operational.

Additionally, only a handful of studies considered were focused on the socio-political and institutional dimensions of blockchain governance (e.g., Wibowo and Yazid (2023) and Radonjić et al. (2024)). While the texts note concepts include digital readiness, bureaucratic inertia, and institutional path dependency, they are seldom thoroughly theorized. Therefore, the literature only provides limited explanations of why technically feasible blockchain programs do not scale in contexts marked by fragmented IT environments, risk averse public administration cultures, or entrenched patronage networks. This dissertation enhances the current literature with an institutional analysis by using an actor-context approach in its analysis. In particular, the dissertation recognizes an interplay of bureaucratic habits, digital readiness, governance culture, and technological readiness to add to blockchain anti-corruption theories, and therefore views technology adoption as a negotiated political process, rather than technical advance.

The also idea of policy transfer, while occasionally referenced in the global pilot's literature (e.g., Gong et al., 2022; Telles, 2022), is also underspecified. Existing literature often assumes that demonstrably successful pilots can be implemented in similarly local contexts across jurisdictions frequently without consideration for contextual asymmetries (i.e., law, regulation, institutional maturity). This dissertation advances understanding of the limitations of policy transfer as a one-way imposition process, and proposes a model of adaptive transfer and scalable contextually relevant cross-jurisdictional learning. The model conceptualizes blockchain adoption as an organic process driven by actors who adaptively learn from cross-jurisdictional experiences. Notably, this model offers a counterpoint the linear, one-size-fits-all narratives often common in contemporary blockchain governance literature: narratives that too frequently ignore the diversity of institutional arrangements which shape public procurement systems across jurisdictions.

In conclusion, the literature we reviewed implies both philosophical framework and empirical legitimacy for this dissertation's main contributions. It confirms that blockchain can be theoretically and practically useful for anti-corruption in public procurement while confirming the field is still underexplored with respect to comparative, institutional, and mechanism-specific matters. The comparative analysis of Italy, Canada, and the USA; the legal–regulatory–technological framework; typology of corruption-risk; and insistence on adaptive policy learning collectively provide a scientifically novel and policy relevant development of this fledgling field.

The literature on blockchain applications for governance and anti-corruption tends to reference pilot test cases, and proof of concept implementations, particularly in the area of public procurement. Though these tests—including the Colombian public contracts blockchain registry, the Brazilian National Treasury's exploration of distributed ledgers, and the pilot e-procurement module in the Emilia-Romagna region of Italy—provide early evidence of technical feasibility, they suffer major deficiencies once better examined in terms of empirical robustness and scalability. Many of the studies are single-case examinations with cases selected for no comparative basis, which constrains their generalizability, or throw out pilot assessments after six months or one year—completely failing to ascertain the long-term operational reliability of the blockchain experiment, the adaptability of stakeholders in its use, or how substitutive corruption might adapt to the new environment.

Furthermore, sample size limitations further limit the empirical weight of many of the claims found in the existing literature. Many pilots consider only the same narrow definitions of procurement categories—in general low-value service procurement, or IT-related tenders— where the volume of procurement is limited and the range of typologies of corruption is dissimilar from high-value infrastructure or security provision, giving rise to the hazard of overstating blockchain's usefulness as a solution when applying findings from individual pilots to a wider procurement ecosystem. Selection bias also appears: the majority of pilots are implemented in jurisdictions or agencies which were already exhibiting above-average political willingness and digital capability; conditions less likely to feature prominently in studies of lower capacity, corruption-prone environments. There is virtually no discussion in the literature of whether the initial successes could pass transfer to low-capacity environments exhibiting weakened institutions or institutional networks supporting procurement capture, entrenchment.

One final area for critiquing existing literature is the blindness towards the constraints on scaling found therein, and the institutional scalability is significantly neglected, while technical scaling (in terms of transaction volume, latency, interoperability) is occasionally acknowledged. Very few studies mention the bureaucratic and political frictions that arise by contemplating trying to scale from narrowly scoped multi-agency platforms to national jurisdictions. Even if they discussed the very concept of operational integrating with the technology options for procurement systems that occupied procurement policy at the time, they generally didn't consider the processes for doing so anything other than potential future planning. Instead, their conceptualizations were generally

over-enthusiastic in their renderings or pre-prototype operating conditions, which amount to grooming moods about being prepared for deployment at better times in the imaginary future.

The evaluation methodologies themselves often lack depth. A great deal of reports emerges from implementing agencies or technology providers with interests, which often leads to selective reporting of successful outcomes while not much emphasis on unresolved issues, going over budget, or user backlash that remains unreported. Generally, independent, academic evaluations are scarce and, when done, are often conducted on self-reported measures from stakeholders involved in the pilot, creating bias that supports a conclusion. In addition, longitudinal data that compiles post-implementation changes in the integrity indicators of procurement, such as the use of competitive tenders or frequency of amendments to contracts, are rarely reported so making it increasingly difficult to know if these changes in transparency are an effective substitute for a decreased risk of corruption.

In comparison (to the broader prod-usage literature), the existing literature typically considers pilots as what they are without documenting them as a mechanism in a more extensive governance system. This approach suggests that the interaction of blockchain-based modules for procurement with anti-corruption measures or supplemental accountability, is not documented (or researched). Other mechanisms relevant to the legal context in which a pilot occurs, such as GDPR in EU jurisdictions where country infrastructures for procurement systems (like Italy) are also fragmented or inconsistent as seen with U.S. state procurement systems.

In consideration of these limitations, for the purposes of this dissertation, the key will be to make a determination and figure a way to accurately and critically move beyond description of pilot initiatives to a mechanism-level critique of their applicability across legal and institutional variations. These considerations mean reviewing how freely available the sample kiwas (as of completion) have been, the accountabilities and evidence to make sense of their discrimination based on misinformation, and in regard to the emerging context of blockchain in the commonwealth's LS2 policies. Studies on blockchain implementations in public political governance tend to mostly draw pilot examples to illustrate the anti-corruption capacity of the technology, many do not even address the basic deficits I have found. First, there is a clear deficit in mechanism-risk fit analysis in academic work. Many pilots - for instance, Colombia's blockchain-enabled public contracts registries, or Brazil's National Treasury's DLT pilots - will reference that they improved transparency at the general level, but do not explain how the construction of the mechanism feature can address specific corruption typologies. For instance, while immutable audit trails can be helpful in addressing risks associated with post-award contract alteration, this risk is distinctly different from unauthorized buried payments, which ought to be characterized as a smart contract; or, a permissioned ledger that restricts insider manipulation of bid evaluations. Since there is no mapped mechanisms and risks along the procurement vulnerability exploitation point, the current literature remains descriptive with no additional operational guidance for implementation of a targeted use.

Second, the lack of focus on actor level resistance limits the explanatory depth to the literature. Even if pilots passed technical assurances, stakeholder resistance can produce a different outcome, but the literature often misses it. In the Emilia-Romagna e-procurement pilot trial the authorities relied on numerous technical assurances - for example, verifiable timestamped on a bid - yet their proximate authorities exhibited resistance since they understood that automation and use of a new technology meant their discretionary impact on a contract would be diminished. Similarly, in Canada, there were internal resistances by the pervasive IT vendors included in their procurement pilots where their fear, or anticipated loss risks, of contracts for the proprietary systems of the IT vendors, despite the blockchain enabled procurement project, and lastly, in the U.S. there is a reluctance by state legislators to be accountable/liable for errors arising from the automation of smart contract execution. In these specific instances, socio-political acceptability is at least as critical as any technical acceptability, and the ideological positioning in procurement ecosystems creates authoritative contexts for adoption trajectories.

Thirdly, most studies are limited by the lack of cross-jurisdictional view of a pilot, which eliminates possible sources around adaptability and policy transfer. In-ground work on blockchain enabled procurement pilots rarely contextualize the asking of exploration, but the variation of legal, regulatory, and institutional differences that shape their design and effectiveness of a pilot. A pilot in Italy noted they needed to adopt either previously adopted EU procurement directive, which encouraged digital standardization, forced GDPR compliance, and when taken together, it created further complication when packaging the notion of a blockchain based immutable ledger. In Canada, the transition authority is fragmented, thus permitting national level digitalization to be deemed a failed undertaking, while in the U.S. the nature of the state-run experimentation policy context, with no state procedural harmonization, or interoperability, fundamentally creates ongoing system, but non-interoperability solutions. Without offered analysis to make comparisons, the preceding examples are either wasted narrative for the literature and/or lack a robust proximate analysis about the qualities that formed a construction of where success or failure where context dependent and what might be uniformly transferable across public governance artefacts throughout jurisdictions.

This dissertation directly addresses these gaps by embedding mechanism-risk fit mapping into the analysis of each case, including an assessments of actor resistance to the implementation in evaluations, and situated all of the findings in a comparative analysis across Italy, Canada, and the United States. This approach means that the examination of blockchain’s potential role in public procurement is not only a technological innovation but a governance reform - subject to institutional constellations, legal cultures, and political economies.

Acting as a proposed mechanism to facilitate transparency and decrease corruption in public procurement, blockchain's narratives have relied on case study accounts, but many of these accounts abstract their case examples from limits of jurisdictional institutions and laws that structure procurement contexts and outcomes. Particularly, while altering public procurement practices through use of blockchain’s immutable audit trails is its most cited mechanism for anti-

corruption, the enabling and constraining factors will differ in all three jurisdictions. In Italy, the legal environment is governed by the Codice dei Contratti Pubblici (Public Contracts Code) and harmonized with EU procurement directives that explicitly note the use of keeping digital records, while being subject to GDPR regulations. This would create a compliance tension between the immutable record keeping and the right to be forgotten, which would require the use of hybrid designs or permissioned ledgers to provide restricted or selective disclosure. In Canada, audit trail mechanisms have fewer impacts from privacy-law conflicts, but face a fragmented procurement ecosystem that each province controls their own procurement statutes and system that makes the interoperability among national systems particularly difficult. In the U.S., which, in terms of procurement law, is a decentralized exercise of governance in federal and state systems, audit trails may be technically simple but the realm of legal admissibility of blockchain records as evidence can vary. Just as for audit trails, a factor for smart contract automation—meant to reduce the opportunity for discretionary manipulation in payments and contract execution—exists in the legal and institutional law structure. Italy's procurement code inhibits discretionary manipulation, but allows limited exceptions, such as for conditional triggers that can be programmed into smart contracts. Implementing or embedding such conditional triggers requires a full understanding of the EU public procurement principles and some form of review or oversight by agencies like ANAC. In Canada, deploying smart contracts requires enduring the differences between provinces' contract laws, especially in terms of enforceability of performance clauses on autopilot. In contrast, the issue in the U.S. on the enforceability of smart contracts often relates to state legislation and courts' interpretation, with a few states including statutory recognition of smart contracts, others remaining silent—all of which culminate in a patchwork of variation that creates an anarchic hindrance for multi-state applications.

The governess of permissioned ledger, used to regulate the validation roles and prevent collusion, is shaped through distinct political economy forces. In Italy, roles for validators could be deployed to public agencies or state-owned enterprises, thus continuation of centralized governance traditions but also pressure for political appointments. Alternatively, consortium models that are public–private, are more common in Canada, instead reflecting the traditions of collaborative governance, though this model also opens door to vendor involvement. In terms of ledger construction, the U.S. has conforming concerns, but with strong open records and transparency laws culture, this transfer to control or restrict the role of validators, in any meaningful way is unlikely.

If we embed these jurisdiction-based contrasts into the analysis of the blockchain mechanisms, this analysis shows distinctly different adoption pathways and risk profile for the same technical feature depending on the legal, regulatory, and institutional context. Highlighting comparative frames supports understanding why pilots that appear similar, result in three different outcomes in three different countries, and provides further evidence for the dissertation's objective of exploring a transferable, context-specific, framework for blockchain-based anti-corruption reforms in public procurement.

The broad review of the literature shows that blockchain's fundamental features of immutability, distributed consensus, traceability and programmable automation, are positioned repeatedly as counter measures to corruption vulnerabilities located in public procurement. The specific technical mechanisms, by mapping mechanisms to risk of specific types of corruption, (e.g. on-chain tender lifecycle management to thwart bid manipulation [Bruschi et al., 2022]; Smart-contract monitoring of compliance checks to limit the potential for re-negotiation of awarded clause as a post-award adjustment [Latha & Chinnaiyan, 2021]; continuous audit protocol to fill oversight voids [Alotaibi, 2023]; tamper-evident ledgers to limit record falsification [Alves Batista, 2024]); in detail present the potential for blockchain, in understanding such traceable records, potentially operationalize transparency and accountability, in a micro-capture way, along the points of highest concern across the procurement process around adding entrenchments for transparency and accountability in formal points of potential or actual manipulation: before (bid submission), during (bid evaluation), after the procurement process (contract award, contract execution and payments).

When these mechanisms are examined in the context of Italy, Canada, and the United States, there are significant differences in how, and whether, they might be adopted and legally recognized. Italy's compliance with EU procurement directives means that there are possibilities for statutory integration of blockchain mechanisms, but there are also concerns about data-protection and the "right to be forgotten" that may not permit full-scale immutability. The fragmented nature of procurement, to the extent that there is an uneven distribution of authority between various tiers of Canada? and interstitial governance failures associated with the lack of interoperability with the many provincial governance structures and authorities, presents an additional difference and challenge, at least as far as privacy law implements less restriction. The United States also has a federal-state architecture that allows for heterogeneity in pilot experimentation, but it also leads to different legal views across the jurisdictions that further complicates problems of scalability and cross-jurisdiction interoperability of blockchain-based records. These challenges illustrate that identical technical designs can face materially and jurisdictionally distinguished adoption pathways, legal views, and governance outcomes.

One further area of limitation in the literature remains the undue conflation of statutory paradigms with regulatory and policy instruments causing "governance" to be treated as a generic category. While some have taken the opportunity to distinguish between legislative powers and administrative regulations, they haven't assessed how these levels interact fully allow (or curtail) blockchain-based statutory or regulatory frameworks in procurement.

This inattention to statutory paradigms also masks basic questions about the permanence, enforceability, or ability to adapt blockchain-based reforms.

Relatedly, the literature does not attend to institutional-readiness and soci-political resistance, although capacity problems, skills gaps, as well as constraints imposed by incumber queries are evidence need to be considered--though seldom in the context of technological feasibility

assessments. Evidence from many different pilot projects in a variety of places insurance that subprocesses types pilots can fail, even if they function at a technical level, if they eliminate institutionally and experimentation based, discretion in decision making, disrupt existing procurement processes, or even displaces established contractor relationships. Concentrating this more properly on the previously-mentioned institutional context expands purely assessing how sub-processes negate counter-corruption that must be considered before sustainable system-wide adoption can take place.

Finally, while international pilot experiences from Brazil, Spain, Colombia, and Peru are useful, the literature almost never considers relevance for jurisdiction with different legal traditions, procurement architectures and political economies. Without a structured approach to contextual adaptation, policy transfer risks over-simplifying into policy with poor domestic fit.

In conclusion, accumulated academic knowledge supports blockchain's possibility in strengthening the integrity of procurement, but its potential varies as it refuses to be successful until legal embedding is careful, therefore, it compared statutory-agency governance instruments distinguishes, to existing institutional calculus, and is cognizant of constraints in some jurisdictions. Therefore, by bringing together the myriad of this lay into an approach to analysis of Italy, Canada and the US, the future for successful mainstream change can hopefully move beyond the proof-of-concept demonstrations toward some coherent contextually relevant framework of anti-corruption reforms enabled by blockchain in public procurement.

Synthesis and implications. With respect to the pilots and conceptual frameworks cited, blockchain's anti-corruption value is derived from its control-layer effect: immutable time-stamping and public verifiability solidify notice integrity; and commit–reveal and automated receipt registers inhibit pre-awarding manipulation; and smart-contract triggers impose integrity on change orders and payments; and append-only audit trails discourage tampering with records. However, benefits observed are tied to non-technical conditions. First, legal embedding—status of records, admissibility of evidence, reversibility/appeal of automated actions, and compliance with data protection considerations—will determine whether on-chain evidence can substantiate oversight and sanctions. Second, governance framework—who the validators are, who sees audit trails, whether any upgrades/overrides are possible, and how exit strategies are defined—will constrain collusion and lock-in with vendors. Lastly, institutional capacity—role-based training, data compatible with OCDS, and legacy integration—will determine if adoption can proceed beyond the pilot stage. This element varies by jurisdiction: Italy's EU-compliant procurement and GDPR compel a more favorable approach to privacy and reversibility; Canada's federated procurement sharply emphasizes the governability of validators and interoperability; and the USA's fragmented arrangements spotlights alignment of standards, record admissibility and appellate review, or safeguards. Thus, we can argue that a blockchain is not a magic bullet but more important as a control architecture, whose efficacy or payoff depends on law, governance, and capacity. We do this operationally in Section 2.4 by mapping—based on Italy, Canada, and the USA—the specific legal preconditions (records, evidence law, data protection rules, reversibility

and appeal), governance arrangements (how validators are assigned, audit rights, whether upgrades/overrides are possible), and elements of capacity in which the same blockchain controls would likely be admissible, enforceable, and sustainable.

To build on these findings, the section that follows compares the relevant legal and regulatory landscapes that set the frame for engaging with the adoption of distributed ledger technologies in Italy, Canada, and the USA. While the preceding section has focused on examining blockchain's technical and governance potential within the procurement workflow, the feasibility and sustainability of implementing these mechanisms ultimately rests on the statutory requirements, regulatory instruments and policy procedure that provide the environment for their operation. To the extent that a comparison exists that purely maps legal environments, further clarify how jurisdictions' specific rules would shape the adoption, enforcement, and legitimacy of blockchain-enabled anti-corruption reform.

This table links each hypothesis to its procurement-lifecycle mechanism (see Table 2.1.1), the corresponding distributed-ledger (DLT) control, and the jurisdiction-specific legal predicates (Italy/EU, Canada, United States) that determine feasibility. It enhances theory traceability by making the literature–mechanism–test pathway explicit and auditable.

Table 3.Table 2.3.1 — Thread Map: Hypotheses, Lifecycle Mechanisms, DLT Controls, and Jurisdictional Legal Predicates

Hypothesis	Lifecycle mechanism (from Table 2.1.1)	DLT control (design choice)	Legal predicates conditioning feasibility (IT/EU • CA • US)
H1: Transparency at publication	Notice integrity and timely disclosure (tender publication).	Certified portal publication plus public hash anchoring; cryptographic timestamp.	IT/EU: BDNCP/PAD under D.Lgs. 36/2023 & ANAC; GDPR storage limitation. • CA: ATIA; Canada Evidence Act ss. 31.1–31.8. • US: FOIA; FAR Subpart 4.5; FRE 901/902(13)/803(6).
H2: Fair access at submission	Bid secrecy, equal timing, and tamper-evident submission.	Commit–reveal; trusted timestamps; threshold decryption at opening; tender-box logs.	IT/EU: eIDAS trust services; Data Act Art. 36 (logging/interruptibility). • CA: PIPEDA; Secure Electronic Signature Regulations (SOR/2005-30); Canada Evidence Act ss. 31.1–31.8. • US: ESIGN; UETA; FRE 901/902(13).
H3: Rule fidelity in evaluation	Criteria/weights integrity; prevention of	Deterministic scoring pipeline with	IT/EU: Data Act Art. 36; eIDAS. • CA: Canada

	off-record overrides in evaluation & award.	human-in-the-loop; signed decision memorandum; immutable logs.	Evidence Act (electronic records). • US: FRE 901/902(13)/803(6).
H4: Contract execution integrity	Change-order abuse, non-delivery, and value diversion during execution.	Milestone evidence (deliverable hashes; inspection attestations); immutable change-order ledger; dual-signature approvals; oracles as needed.	IT/EU: eIDAS; GDPR (off-chain PII; on-chain commitments). • CA: PIPEDA; Secure Electronic Signature Regulations. • US: ESIGN; UETA; FRE 803(6).
H5: Payment integrity and close-out	Phantom/duplicate payments, concealment of late payments, mismatch of deliverables.	On-chain three-way match (PO–GRN–invoice); signed payment authorization; retention-aware evidence bundle; FOIA/ATIA-ready export.	IT/EU: BDNCP/PAD continuity; GDPR retention. • CA: ATIA; Canada Evidence Act ss. 31.1–31.8. • US: FAR Subpart 4.5; FOIA; FRE 901/902(13)/803(6).

Table Note. *Legal predicates cover statutory publication channels, trust-service/signature regimes, evidence rules for electronic records and automations, and data-protection constraints by jurisdiction. Controls are expressed as auditable artifacts (e.g., signed receipts, hash-anchored logs, bid-opening transcripts) to enable reproducible verification by auditors and courts. The integrity-layer approach keeps personal data off-chain while recording on-chain commitments (hashes, timestamps, signatures) to preserve probative value.*

The Thread Map provides a framework for written literature on the corruption mechanisms, including some testable propositions, which identify each hypothesis to lifecycle mechanism, specific distributed-ledger controls and the law, which makes each a control admissible, enforceable in Italy/EU (that illustrates both regime) Canada, and the United States. In short, the first hypothesis connects statutory publication on official portals with public hash anchoring to increase notice integrity, the second connects a commit and reveal protocol with trusted timestamps and threshold decryption to veil bid secrecy and timing, the third connects deterministic scoring pipeline with logged actions and signed decision memorandum for review, the fourth connects contract execution via an evidence bundle of milestone and a chang-order ledger, which cannot be corrupted, and the last connects integrity at payment and close-out with on-chain three-way-matching and disclosure-ready evidence bundles.

This mapping also helps establish construct validity by making visible the auditable outcomes—publication receipts exposing timestamping, sealed-bids commitments/commitment abstractions (noting not everything is embedded in the contract), transcriptions of sealed bid opening practices, logging of outcomes of deterministic scoring, evidence bundles of milestones, proof of three-way-matching—for each the control component element, with disruptive events noted via smart

contract. All of the artifacts above could visible and reproducible by an auditor: re-computing a hash, trusted timestamps, proving a signature, validating portal receipts, or reconstructing a timeline.

The key in developing the controls with these recently developed electronic-records and self-authentication regime, the requirements for identity and signature by state and territory, provided mechanisms that can be leveraged to reducing the separation between technical and assurance credibility, and evidence thresholds.

The design is purposely hybrid. A permitted ledger is used as the system of record to capture and control the requirements of confidentiality, throughput and access-control, periodic hash-anchors to a public chain provide independent timestamps and electronic evidence of corruption. The governance and risk management controls—independent moderation and oversight, methods for controlling changes, testing for exits and portability, and bundled evidence—provide navigated consortium risks and provide an ability to unprocessed and provide a due process. Some of the jurisdictional. Customary and subnational rules will likely need to be customized, together with the risk of an oracle or performing the required software updates for the smart contract, a layer of integrity system which also maintains user tags, allows for personal data to permanently remain off-chain while the verification of on-chain commitment happens, can assist to minimize probative value and meet data-protection obligations.

Overall, the Thread Map can mitigate HARKing risk by pre-committing the logical sequence of what it is demonstrating in the underlying literature from mechanism to propositions to test, and structure for maintainable groups to enable comparative research and evaluation systematically.

2.4 Comparative Legal and Regulatory Landscapes for DLT (General)

Table 4.Table 2.4.1 provides a cross-jurisdictional overview (Italy/EU, Canada, U.S.) of the specific legal and regulatory parameters that directly constrain DLT design choices in public procurement.

Topic	Italy / EU	Canada	United States
Data protection & retention	GDPR limits personal data retention to what is necessary. In Italy, procurement publication and	PIPEDA requires limiting use, disclosure, and retention to what is necessary (S.C. 2000, c. 5, Sch. 1, Principle 4.5).	The U.S. has no omnibus federal privacy law. Records management follows OMB/NARA guidance

	retention are managed via the BDNCP under D.Lgs. 36/2023 and ANAC Delibera 263/2023	Federal access to records is governed by the Access to Information Act (R.S.C., 1985, c. A-1).	(M-23-07), and public access is governed by FOIA (5 U.S.C. § 552).
E-signature & smart-contract status	eIDAS confers handwritten-signature equivalence on qualified e-signatures and, as amended, creates the EUDI Wallet (Regs. 910/2014; 2024/1183). The EU Data Act requires core safeguards for smart contracts used in data-sharing agreements (Reg. 2023/2854, Art. 36).	Electronic signatures are recognized under PIPEDA, Part 2 (Electronic Documents) and the Secure Electronic Signature Regulations (SOR/2005-30). Evidentiary treatment of electronic documents is set out in the Canada Evidence Act (ss. 31.1–31.8), while most provinces implement the Uniform Electronic Commerce Act (UECA).	Functional equivalence is provided by the ESIGN Act and state enactments of the UETA. There is no federal smart-contract statute; enforceability is generally addressed under state contract and evidence law.
Public-records & evidence rules	Legal publication and data transmission in procurement flow through BDNCP under D.Lgs. 36/2023 and ANAC Delibera 263/2023, including transmission to the EU Official Journal (OJ).	Access to federal records is governed by the Access to Information Act; authentication/admissibility of electronic records is addressed in the Canada Evidence Act (ss. 31.1–31.8).	Public access is under FOIA; admissibility and authentication rely on FRE 901, 902(13) (self-authenticating electronic records), and 803(6) (business records).
Procurement-specific e-tendering rules / platforms	Italy mandates digital procurement via certified PAD interoperable with BDNCP; since 1 Jan 2024, PAD/BDNCP is the default publication and lifecycle channel (D.Lgs. 36/2023; ANAC).	Federal e-tendering is conducted through CanadaBuys (SAP Ariba) under Public Services and Procurement Canada policies (PSPC Supply Manual).	SAM.gov is the government-wide point of entry; FAR Subpart 4.5 recognizes electronic commerce in contracting.
Digital-identity frameworks	The trust-services regime under eIDAS and the eIDAS 2.0 amendment establish cross-border high-assurance	The Pan-Canadian Trust Framework (PCTF) developed by DIACC supports interoperable identity assurance. Operational credentials	NIST SP 800-63-3 defines IAL/AAL/FAL for federal digital identity; Login.gov provides IAL2-compliant identity

	credentials, including the EUDI Wallet.	include GCKey; Treasury Board provides MFA and credential-assurance guidance.	proofing for participating agencies.

Note: GDPR=General Data Protection Regulation; eIDAS=electronic Identification, Authentication and trust Services; BDNCP = *Banca Dati Nazionale dei Contratti Pubblici*; PAD = *Piattaforme di Approvvigionamento Digitale*; PIPEDA = *Personal Information Protection and Electronic Documents Act*; ATIA = *Access to Information Act*; ESIGN = *Electronic Signatures in Global and National Commerce Act*; UETA = *Uniform Electronic Transactions Act*; NIST SP 800-63-3 = *Digital Identity Guidelines*.

As summarized in Table 2.4.1, these legal determinants translate into concrete DLT design constraints for public procurement across the three jurisdictions.

The comparative matrix identifies the legal determinants that most directly translate into system-level design constraints for distributed ledger technology in public procurement, focusing methodologically on five interrelated clusters: (1) protection and retention of procurement-related personal and commercial sensitive information; (2) formal requirements for signatures and automated action enforcement; (3) admissibility/disclosure of electronic records; (4) platform rules identifying authoritative points of publication and submission; and (5) identity-assurance regimes determining who can bind the state or suppliers. The goal is to do more than "comply" but to design an on-chain data structures and workflow logic that is legally cognizable, evidentially-rich, auditable across jurisdictions.

Regarding data protection and retention, the EU/Italy regime, which relies on the storage-limitation and purpose-limitation principles of the GDPR, prohibits indefinite on-chain storage of personal data and encourages architectures that externalize raw data to controlled storage repositories that anchor integrity on-chain. Good designs then enable off-chain storage with on-chain digital assets (e.g., hashes) that documents intended retention schedules at the repository layer with mechanisms to either revoke or restrict access as lawfully permitted. Canada's PIPEDA maintains a similar limiting-retention principle, and along with the Access to Information Act, promotes strong provenance, versioning, and data trails that are ready for disclosure. There is no all-embracing federal privacy statute in the US, but that does not entail a loosening of constraints: records-management obligations (e.g., OMB/NARA policies) and FOIA disclosure minima require lifecycle measurements and reproducible audit trails. Across all three jurisdictions, the prudent design position is to consider the ledger an integrity layer, and limit identifiable data storage to highly controlled, off-chain stores.

In terms of e-signatures and smart contracts, the EU regime (eIDAS), coupled with Data Act design-level safeguards for smart contracts applied in data-sharing contexts, supports

permissioned deployments that enact controlled termination ("kill-switch"), role-level access, and a complete logging of events. Canada and the US maintain functional-equivalence regimes (PIPEDA/UECA; ESIGN/UETA) that permit digital execution if integrity, accountability, and informed consent can be demonstrated. In all three case systems, a sound engineering practice is to externalize signature creation and identity proofing to trust-service providers or government identity regimes, keeping verifiable proofs (e.g., qualified seals, signed assertions) on-chain, and document the verification process to buttress enforceability and non-repudiation.

Public-records and evidentiary norms shape the probative weight of ledger outputs, and the circumstances of disclosure. Italy's BDNCP serves as the legally established route for a legally sanctioned channel for publication and data collection across the procurement lifecycle, and is a fortuitous point of integration for DLT-based integrity services (e.g., anchoring of tender notices, bids, and award data). In Canada, the electronic documents provisions of the Canada Evidence Act can yield a predictable acceptance path in court where system reliability, integrity controls, and the chain-of-custody can be evidenced; Access to Information obligations serve to further motivate reproducible audit trails, instantiating time and author details for any records. In the US, the Federal Rules of Evidence – specifically the authentication (FRE 901), the self-authentication of electronic process records (FRE 902(13)), and the business records exception (FRE 803(6)), favor architectures that yield certifiable technical logs, immutable timestamps, and reproducibility in an export form.

Ultimately, procurement-platform rules and identity frameworks constitute the operational surface through which all DLT elements must interoperate. Italy's certified PAD/BDNCP ecosystem, the CanadaBuys (SAP Ariba) for Canada, and the U.S. SAM.gov/FAR environment, as identified above, are the authoritative endpoints for publication, submission, and lifecycle data. Therefore, DLT will be most useful as an integrity and audit layer – publishing irreversible commitments, automating milestone validations under clearly scoped conditions, providing persistent evidence of verifiability—rather than a wholesale replacement of existing platforms. Identity frameworks (e.g., the EU's EUDI Wallet, Canada's PCTF or GCKey, and the U.S. Login.gov aligned with NIST SP 800-63) set assurance levels for enrollment and binding actions; substantial implementations bind transactions to high-assurance credentials and retain attestable proofs (e.g., qualified electronic seals or IAL2 assertions) to guarantee evidence and compliance benchmarks are met. Through this layered approach (platform integration, identity assurance and evidence quality), we can provide a jurisdictionally-sensitive blueprint for the adoption of DLT solutions in public procurement in a feasible and legally durable manner.

The global legal and regulatory ecosystem around blockchain and distributed ledger technology (DLT) has flexibly and rapidly adapted to the existing limitations of identifying and distinguishing new opportunities and innovations from the existing obligation to protect the public interest—such as privacy, market integrity and financial stability. This comparative lens indicates that the European Union has developed its best practices as a leader in harmonizing regulatory action through the General Data Protection Regulation (GDPR) and the Markets in Crypto-Assets

(MiCA) Regulation, and integrating actions focused on data protection with ongoing efforts to regulate blockchain and digital assets, and virtually associated financial innovations (Akanfe, Lawong, & Rao, 2024; Maume & Kesper, 2023). This comparatively balanced work in Europe brings together the fundamental ideation, governance and action around digital, and shows extremely high levels of observation and related governance innovation across all aspects of DLT (operational platforms; market; role; use case; use cross-functionally etc.) (Akanfe, Lawong, & Rao, 2024; Maume & Kesper, 2023). In very contrast, the United States has adopted a de-centralized and fragmented approach to governance innovation and established overlapping, potentially conflicting jurisdiction of any number of federal and state authorities, such as the Securities Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Financial Crimes Enforcement Network (FinCEN) (Chadaeva, 2024; Yeoh, 2017). Adams (2024), adds that Canada is in between the fragmentation and case-by-case escalation, where many decentralized (provincial) regulations are emerging, but clearly driven by centralized policy at the national(federal) jurisdiction which allows for a degree of scope of autonomy, but subsequently lacked clarity, predictability and stability (Ducas & Wilner, 2017; Selvanesan & Rodrigo, 2024).

The differences in regulatory proximity and philosophies, between the U.S. and Canada, are visible through different paths toward blockchain application and compliance within Italy, Canada and the U.S. Although Italy is navigating these changing complexities and issues in the EU's integrated policy framework, the EU has established legal clarity with a harmonized framework, developed to be responsive to the EU's high data protection standards. Although still contending with the challenges of addressing data immutability, the un-permissioned regulation(s) of blockchain ledgers, decentralization and locally working jurisdictions, and total ownership of data. Though the EU established a legal certainty with its harmonized framework, that allows for framework-based implementation out of legal clarity—and without consideration for operationalization of diverse and differing leaded DLTs. Article 17 of GDPR provides the right to erasure to subjects, thus introducing tensions between database ledger's permanent, transparent and immutable features, and the evolving community rules for the immediate future of technology in encryption and developing sporadic practices around erasure and even data minimization (Ibáñez, O'Hara, & Simperl, 2018; Dutta et al., 2020). Because the U.S. lacks a national/provincial federal data protection statute, implementing state-based distributed data protection, and unique -yet fragile state level- data protection regulations like California's Consumer Privacy Act (CCPA), or limited regulation around the other sectoral data protection statutes (e.g., HIPAA), U.S. developers and users experience uncertainty, but also face greater flexibility (Zafar, 2025; Herian, 2020). Canada has enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) to enable more compliance freedom in developing a holistic regulation with consideration of other regulations at both the national and provincial level, yet similar implementation to the foundational principles remains problematic, especially for un-permissioned services (Campanile et al., 2021; Zafar, 2025).

In the European Union (EU), the creation of blockchain regulation has been based on harmonization and legal certainty with tools like the General Data Protection Regulation (GDPR) and Markets in Crypto-Assets (MiCA) Regulation. The tools of regulation represent a joined-up effort to manage innovation in blockchain in accordance with fundamental rights, market integrity, and cross-border interoperability (Maume & Kesper, 2023; Blemus, 2018). However, Italy, which is part of the EU acquis, represents national adoption of the same supranational legal logic which incorporates regulations into national legal systems in areas such as vertical and horizontal data protection and financial market supervision (Kamalyan, 2020; Cappai, 2023). The GDPR is the widely accepted global standard for data privacy, but the GDPR has instantiated structural tensions with the core design principles of blockchain - as shown by immutability and decentralization. Legal rights of modification and erasure (Articles 16 and 17 GDPR) conflict with the concept of append-only state in a distributed ledger, and the issue has been extensively debated in academia as to whether GDPR is compatible with the native blockchain (Berberich & Steiner, 2016; Ibáñez, O'Hara & Simperl, 2018).

Subsequent proposals to address the tensions are mixed technical–legal strategies. Scholars and regulators, have proposed to use off-chain data storage (to use hashed pointers to blockchains), advanced encryption methods, or relying on zero-knowledge proofs to restrict personal data used on-chain to the highest degree possible (Akanfe, Lawong & Rao, 2024; Dutta et al., 2020). These strategies are a part of Shadow blockchain and are also being undertaken in practice as Italy is also participating in the EU DLT Pilot Regime as an experimental regulatory framework. The regime provides supervised testing of blockchain-based trading and settlement infrastructures under time-limited regulatory relief and thus allows innovation while gathering empirical evidence to inform definitive legal frameworks (Maume & Kesper, 2023). Scholars have pointed to this approach as a case of “participatory regulation,” where legal frameworks are iteratively refined through stakeholder engagement with the technology and institutional learning (Cappai, 2023; Faria, 2023).

In contrast, the regulatory landscape in the United States is characterized by fragmentation, including a plural institutional environment for regulation. Regulatory authority over digital assets is shared among a range of federal regulators, including the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and the Financial Crimes Enforcement Network (FinCEN), that apply distinct legal standards according to their agency mandates (Yeoh, 2017; Chadaeva, 2024). This produces a substantial degree of uncertainty in interpretation, particularly regarding the classification of digital tokens according to law as securities or commodities, and the definition of DeFi applications, and increasingly convoluted by state-level regulatory developments like New York’s BitLicense framework, which imposes heavy regulatory compliance obligations upon virtual asset businesses (Ng, 2025). The absence of a coherent federal data protection statute, such as GDPR-style legislation, further adds complexity to governance arrangements, and leaves data privacy issues for resolution through sectoral laws (eg HIPAA, GLBA) and spatial laws like the California Consumer Privacy Act (Zafar, 2025; Herian, 2020).

Thus, developers and users of blockchain technologies in the US is confronted with a limited landscape of fragmented and inconsistent standards that produces hurdles to cross-jurisdictional scalability and legal certainty.

Canada's legal and regulatory stance for innovative uses of distributed ledger technologies occupies a middle ground between the EU's centralized harmonization and the US's fragmented institutionalism. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) is foundational to Canada's data privacy regime and shares many of the same conceptual foundations with GDPR, like informed consent, purpose limitation, and data minimization (Campanile et al., 2021; Zafar, 2025). Unlike the GDPR, PIPEDA allows broader discretion in interpretation and enforcement, allowing regulators to explore a more flexible stance toward using emerging technologies -- including contextualizing blockchain deployments with sectoral compliance regimes, especially in finance and the delivery of government services (Ducas & Wilner, 2017; Ellul et al., 2020).

The dual-layered governance structure which typifies the Canadian regulatory model comes largely from the premise of federal control and domain over anti-money laundering (AML) and privacy, while provinces\sectors are responsible for other aspects, such as securities and consumer protection, etc. For example, while the Office of the Privacy Commissioner of Canada supervises PIPEDA at a national level, federally as well as at the provincial level securities regulators, such as the Ontario Securities Commission, share authority via jurisdiction defining the lawfulness of digital assets and token offerings (Selvanesan & Rodrigo, 2024; Chadaeva, 2024). The regulatory disaggregation structures provide somewhat overlapping yet, layered oversight structures which scholars have suggested may be the right path for regulatory innovation or may offer new entrance barriers to the market, depending on the quality of coordination (Ducas & Wilner, 2017).

Canada's regulatory interaction with blockchain has included sandbox models and public consultations, which have allowed Canadian institutions to explore the risk and utility of blockchain technology and its applications for {digital} identity, or transfer payments, and other human activities. Although there is not an overarching national strategy as there is in the EU's MiCA, there has recently been a greater willingness of Canadian regulators to identify digital tokens as securities and disclose, register and offer service on those registries (Ng, 2025; Roy, 2023). Additionally, there are many problems that remain in the regulatory categories of governance in DeFi, enforceability of smart contracts, and lack of statutory definitions of blockchain components that exist at a consideration of continuing discord around regulation globally. As scholars have recognized in both the EU and the U.S., Canada has a more difficult but comparable harmonizing context, especially if regulations and harmonization of international data flows and cross-border financial services develop with blockchain as part of that graven and insistent data challenge (Zhuk, 2025; Blemus, 2018).

A continuing part of the challenge everywhere - Italy (EU), Canada and the United States - is to find some way to reconcile blockchain's decentralized structure with appropriate and acceptable

privacy and digital rights regimes, which are what exist today. For example, in the EU, under the GPDR requirements, the data controller must be responsible for compliance, including requirements of purpose specification, minimizing data, and ability to amend or to delete personal data upon request, that directly counter the attributes of use of permissionless blockchains where data is OK and/or cannot be deleted or establish basis for modification (Berberich & Steiner, 2016; Tatar et al., 2020). Blockchains have begun to explore design issues that are regulatory-compliant, for example putting personal data off-chain while relying on hashed references of or pseudonymous identifying information on-chain, while preserving the utility of the ledger, yet comply with the legal obligation to recognize personal data as indicator of regulation (Ibáñez et al., 2018; Dutta et al., 2020).

In the case of Canada, similar tensions exist under PIPEDA, which reflects the right of withdrawal of consent, while also requiring organizations to be able to demonstrate the accuracy and security of personal data. PIPEDA is not as prescriptive as the GDPR, but it poses a challenge for blockchain developers to think deeply about how to develop architectures that allow users to control their data without compromising decentralization (Campanile et al., 2021). In practice, Canadian regulators have exhibited a more principles-based approach, examining the blockchain deployment on a case-by-case basis, and enabling it through regulatory sandboxes and pilot projects to install innovation (Ducas & Wilner, 2017; Selvanesan & Rodrigo, 2024).

The United States is different, as there is a lack of an overarching federal data protection regime, which leads to a much more complicated situation. While laws like the California Consumer Privacy Act (CCPA) impose minimum protections for data, they simply do not establish enforceable rights as individuals have with respect to the GDPR to access, erase, or port their data (Zafar, 2025; Herian, 2020). Therefore, while this fragmentation appears to allow for more experimentation around blockchain architectures, it also raises a number of potential legal vulnerabilities, specifically concerning data transfers/processing in other jurisdictions and consumer-based blockchain implementations. According to Zafar (2025), the absence of coherent federal privacy framework makes assessing whether a particular blockchain application is compliant virtually impossible. They go on to suggest that ultimately this has created a regulatory void that could be limiting more than just innovation, but the long-term scalability of blockchain overall, as well as subsequently eroding trust. The comparative literature therefore highlights the need for international harmonization around principles of core data protection, as blockchain applications develop in areas such as health-integration security, identity verification, and public procurement systems (Faria, 2023; Akanfe et al., 2024).

In addition to prevalent differences in regards to data privacy, a second and equally significant and pervasive axis of difference in legal perspectives on blockchain systems in Italy (EU), Canada, and the United States concerns the issue of regulating digital assets which includes cryptocurrencies, stablecoins, and tokenized securities. The MiCA Regulation passed by the EU is the most

ambitious regulatory initiative in the world to try and define and regulate crypto-assets under a legal umbrella. MiCA classifies crypto-assets into categories including e-money tokens and asset-referenced tokens, and establishes licensing, capital and disclosure obligations for service providers (Maume & Kesper, 2023; Faria, 2023). Italy has begun implementing transitional regulations compliant with its MiCA obligations, while also exploring regulatory innovation at a national-level using participatory models (Cappai, 2023). In conjunction with the DLT Pilot Regime, Italy, rather aim to capture risks to the systems, while enabling an environment conducive to innovation in capital markets infrastructure.

Conversely, the United States remains challenged by definitional ambiguities at the underlying level. Federal bodies have different definitions for digital assets; for example, the Securities and Exchange Commission (SEC) is inclined to characterize many "tokens" as securities in terms of the Howey Test, while the Commodity Futures Trading Commission (CFTC) takes the position that it has jurisdiction over the remainder as commodities. Most recently, regulatory dualism has been implicated in generating conflicting enforcement actions, and rhetorical uncertainty—regardless of the regulatory defensive actions—occupies valuable cognitive resources for issuers, investors and developers (Yeoh, 2017; Chadaeva, 2024). While there have been some products which did suggest an alternative—such as the SEC's Framework for "Investment Contract" Analysis of Digital Assets—these products provide guidance, but they do not have the authority of statute and do not provide definitive conclusions to significant definitional and substantive uncertainties regarding utility tokens, custodianship, or decentralization in the context of an offering (Ng, 2025). There also exist various inconsistencies among states which generates regulatory uncertainty, and creates significant compliance obligations for each jurisdiction (Roy, 2023).

For Canada, a slowly skeptical yet practical path has evolved. While existing legislation does not have the scope of MiCA, Canadian securities regulators have moved quickly to assert oversight over crypto-asset trading platforms and token offerings. In guidance from the Canadian Securities Administrators (CSA), it has been confirmed that securities laws have jurisdiction over digital assets unauthorized as securities, where the contract is created under existing Securities laws, and that registration is needed for platforms that are providing these assets to the public (Ducas & Wilner, 2017; Selvanesan & Rodrigo, 2024). This ensures that there is protection for investors but has also sparked debates about the viability of using existing legal constructs to fit new blockchain models.Scholars explain how Canada has a multi-layered regulatory system based on cooperative federalism, which creates opportunities for innovation on the public policy front. But also creates possibilities for overlapping jurisdictional claims if inter-agency activity is not coordinated (Zhuk, 2025; Blemus, 2018).

The regulation of asset tokenization, in which physical or financial assets are represented digitally on a blockchain, may be further illustrative of the legislative innovation (or lack thereof) and regulatory agility that is present in Italy (EU), Canada, and the United States.

Within the EU, MiCA and the DLT Pilot Regime are establishing a legal framework for asset tokenization by clarifying operational, custodial, and compliance requirements for tokenized financial instruments. This has given market participants the ability to issue and trade securities on distributed ledgers, in a regulated environment promoting financial inclusion, market efficiency, and systemic risk mitigation (Maume & Kesper, 2023; Jūrmalis, Berķe-Berga, & Urbāne, 2025). In Italy, they have structured their national ecosystem to embrace these supranational obligations, with additional provisions for experimental governance methods, such as hybrid public–private partnerships to test blockchain for securities settlement, public procurement, and digital identity systems (Cappai, 2023; Kamalyan, 2020).

Canadian regulators have seen asset tokenization as an increasingly novel financial modernization avenue. And while no statutory definitions exist for tokenized asset classes in Canadian law yet, regulators have acknowledged the technological and economic viability of tokenization in capital markets, especially for small and medium-sized issuers (Ng, 2025; Roy, 2023). On the regulatory side, the Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) have jointly published guidance indicating that current securities frameworks will extend to digital assets such as tokenized debt instruments and equity shares. This demonstrates a preference for continuity in regulation over legislative reform and, therefore, leave regulators and the markets the flexibility to consider innovation within existing frameworks and reduced disruption (Ducas & Wilner, 2017; Selvanesan & Rodrigo, 2024). Still, scholars have noted challenges which arise from a responsive strategy resulting in interpretive gaps, and differential treatment from region to region, particularly for emerging governance structures (and regulatory challenges) such as decentralized autonomous organizations (DAOs), or smart-contract trading (Zhuk, 2025).

In the U.S., asset tokenization has been of such notable interest from market innovators and regulators that it is currently a regulatory 'mess' both in terms of how it will be treated legally and its undeveloped rapport with systems of legal interpretation and regulation. The SEC has taken a lead role in determining that many tokenized assets are securities that issuers must ensure compliance with pre-registration and disclosure requirements from the Securities Act of 1933. But regulators have remained silent on aspects related to token custody, the automation of compliance, or the enforceability of the terms of smart contracts (Chadaeva, 2024; Yeoh, 2017). Additionally, participants in asset tokenization must comply with overlapping obligations from the SEC, CFTC, and numerous state agencies. The passage of regulatory obliques takes shape in a highly fragmented space, which in turn is often filled with a risk-averse approach to regulatory developments. Legally while asset tokenization is considered an innovative and transformative technology, the growth potential of asset tokenization is narrowly constrained by structural regulatory fragmentation, as well as a lack of formal legal acts or regulations that encompass the various complexities that accompany DLT base financial instruments (tokens) (Ng, 2025; Noble, 2020).

One aspect of a convergence in regulation across Italy, Canada and the U.S. is the governance of financial risks, particularly built around anti-money laundering (AML) compliance, consumer protection and addressing systemic risks, in relation to blockchain-based finance systems. In general, financial risks will remain at the forefront of legal innovation on DLT regulations, as jurisdictions balance enforcing the apparent need to protect public safety and market integrity with innovation associated with more competitive capital markets. Within the EU, the AML obligations for VASPs were established in the EU's Fifth and Sixth Anti-Money Laundering Directives, which build AML obligations requiring crypto-asset intermediaries to have knowledge of some level of KYC in the context of reporting significant AML issues in relation to AML and transaction monitoring practices. The obligations within the AML VASP regime were also reflected in Italian, where Italian authorities have similarly acknowledged their own guidelines to build on aspects such as risk-based supervision, and the need to maintain a coherent and similar regulatory approach with the existing EU standards, for financial governance (Kamalyan, 2020; Cappai, 2023).

MiCA is going to also intensify AML expectations, requiring crypto-asset issuers, custodians and exchanges to have internal processes to control, document, assess, and control risk exposure, operational resilience, and understand customer due diligence. This is an explicit legal shift to active compliance management from passive compliance management, and highlights financial integrity as a pivotal aspect of the structural aspects of DLT regulation (Maume & Kesper, 2023; Faria, 2023). However, legal scholars are still debating whether or not DLT frameworks that they have crafted address new risk channels associated with the emergence of decentralized finance (DeFi) and algorithmic trading systems, that rely solely on financial algorithms, rather than any identifiable legal entity exercising any reasonable level of financial discretion (control) (Barbereau & Bodó, 2023).

Canada, has taken a similarly strong approach. FINTRAC administers/a regulatory Aml Compliance regime for the digital asset industry, while provincial regulatory bodies, have also create rules (guidance) regarding custody, transparency, and operational risk. The Canadian regulatory policy needs around 'functional equivalence' has been the fundamental context for applying existing financial statutes to services provided only operating on blockchain technology (i.e., for services with the same activity not with a technological approach) (Ducas & Wilner, 2017; Selvanesan & Rodrigo, 2024). Yet, similar to Italian examples, as Canadian legal scholars recognized some of the potential issues resulting from Canada's reliance on principles-based regulation is that the regulators may become stymied by the fast pace of potential changes characteristic of permissionless systems that may not rely on traditional forms of compliance systems (account verification or transaction freezing) (Zhuk, 2025; Zafar, 2025).

The United States (U.S.) regulatory environment similarly emphasizes AML and consumer protection, whilst contending with overlapping jurisdiction and enforcement in conjunction with other regulatory competition. Hence, FinCEN has taken the lead requiring crypto-asset platforms to register for AML and the SEC and CFTC take enforcement action against unregistered securities and market manipulation. However, scholars often criticize the U.S. regulatory model as fronted

by an enforcement agenda aggravates fragility in the law and regulatory chaos, as well as potentially discourages any incentive to comply (Chadaeva, 2024; Yeoh, 2017). In addition, and critically, there are no formalized consumer protection laws directed at smart contracts and decentralized applications, leading to an increased risk of fraud, misrepresentation and deficiencies in technology without a legal instrument to support them (Ng, 2025; Roy, 2023).

A growing literature identifies the emergence of experimental, and participatory regulatory approaches needed to reflect the complex and developing nature of blockchain technologies. Many throughout the EU, and specifically in Italy, have started to call for flexible regulation with legal scholars emphasizing the ability to regulate by way of example regulations, legislative sandboxes, and public–private co-regulation projects (Cappai, 2023; Faria, 2023). Where the EU has made some strides in the field of regulation, with the DLT Pilot regime permitting select financial market participants to test blockchain-based trading and settlement infrastructures in a controlled environment and with lessened regulatory implications, all under the watch of National and EU regulators. Italy has taken an enthusiastic approach to this framework, using it to conduct experimentation with regulatory improvements in procurement, digital identity, and registry management, and align national experimentation with supranational objectives (Kamalyan, 2020; Maume & Kesper, 2023). These policies are built upon the idea of 'participatory regulation', which involves multiple stakeholders (regulators, developers, legal academics, and end users) in the design and assessment of the regulatory framework in an iterative approach. This dynamic model of regulation is consistent with a project and areas of innovation, like blockchain technology, where legal codes can quickly be outdated or even counterproductive (Barbereau & Bodó, 2023). Participatory regulatory frameworks offer regulators opportunities to learn from the way in which legal codes are applied in practice, adjust regulatory oversight mechanisms, and co-create standards with industry in a controlled and evidence-based way (Faria, 2023; Cappai, 2023).

This articulation of regulation has produced new governance arrangements in Italy that blur the lines of hard law, soft law, and self-regulation. These arrangements are particularly prescient in high-impact environments like financial services or government transparency.

In Canada, experimentation with regulatory sandboxes is beginning to take hold, primarily through agencies like the Ontario Securities Commission and the British Columbia Securities Commission. For example, regulatory sandboxes allow blockchain startups to use temporary exemptions while regulators contemplate the potential consequences of emerging business models (Selvanesan & Rodrigo, 2024; Ng, 2025). Although Canada is diplomatic and cautious, it is an acknowledgment of increasing institutionalization that legal certainty must be balanced with regulatory flexibility to define innovation, and prevent regulator and regulatory by way (Zhuk, 2025). Opponents warn that the outcomes of sandboxes may become merely anecdotal, in absence of success measures, and greater legislative context, that may prevent reform (Roy, 2023).

In contrast, the United States has taken a more hesitant route with participatory or experimental expressions at the federal level. State governments, for instance, Wyoming has been more

participatory, with legislation, but Federal Agencies have demonstrated a predominant view toward ex post enforcement rather than regulatory experimentation ex ante. This regulatory position may either indicate a reflection of institutional inertia or an explicit option to preserve a degree of regulatory flexibility, but it also raises questions regarding transparency, legal certainty, and the feasibility and scalability of compliance mechanisms in decentralized and emergent situations (Zafar, 2025; Herian, 2020).

While there are notable jurisdictional differences in institutional frameworks and legal paradigms, similarities are emerging in the rapid conformation of distributed ledger technologies. Italy (EU), Canada and the United States are all converging in their appreciation for legal certainty through the ability to define digital assets, protect consumers and investors, and apply blockchain within regulated financial and public systems. New examples are emerging in the slow journey towards the normalization of DLT applications for digital identity verification, supply chain verification, and public procurement – sectors where transparency, auditability, and legal enforceability are necessary (Faria, 2023; Cappai, 2023).

In the EU, regulatory experimentation with blockchain has become more integrally linked to broader digital governance policies, seeking to introduce blockchain as a tool to improve government accountability and to mitigate corruption. Italy has engaged in EU contributions to investigate the application of blockchain in various forms, including document verification, procurement verification, and in the automated auditing of public contracts, aiming to comply with the regulatory requirements of the GDPR and complying with MiCA (Kamalyan, 2020; Maume & Kesper, 2023). Such examples are about more than just legal innovation; they demonstrate an institutional commitment to improve the capacity in which states can deliver services while maintaining legal safeguards. Academics examining these developments have noted in their analysis that say immutable and traceable blockchain offerings can provide secure layers of integrity, however must be countered with further considerations on data processes pursuant to the data security obligations of public authorities and respective added layers of rigidity of administration (Ibáñez et al., 2018; Tatars et al., 2020).Canada has also shown some interest in utilizing blockchain technology to support public service efficacy, but it has been done in a much less coordinated manner. Federal and provincial authorities are liaising with private actors to pilot blockchain-based applications in areas such as digital credentialing, land registries, and financial disbursements. However, academic commentators have emphasized the lack of a more general cut strategy for blockchain uptake in Canadian public institutions has made adoption variable practice, risk management, and data governance (Selvanesan & Rodrigo, 2024; Zafar, 2025). The issue was complicated by the lack of statutory recognition for smart contracts and tokenized rights in the context of legally binding procurement processes, although the regime of principle-based regulation provides some latitude of interpretation (Ducas & Wilner, 2017).

Blockchain has had a very experimental application in the USA's government space as it is still very much in a process of development by agency's mandates. Work from the Department of Homeland Security, and state examples of ex., procurement tracking and voting systems have

pointed to the promise of blockchain ecosystems, but also the legal risk of being able to meet existing regulatory frameworks in a viable way (Chadaeva, 2024; Herian, 2020). Yet without a cohesive federal strategy for blockchain to be integrated fairly specifically into the public sector in a possible or practical way, not surprisingly attempts at developing blockchain remain isolated and vulnerable to administrative change, particularly as contracting, data interoperability, and customers' rights remain binding in some way (Ng, 2025; Roy, 2023).

Legal enforceability is ultimately at the center of cross-regulating debates involving blockchain and especially on the topic of smart contracts and automated execution systems. We are seeing from the perspective of legal scholars that in Italy, Canada, and USA, we are seeing challenges in whether it is possible for current doctrines of contract law to be adapted to chain logic where a computer tier may escalate transaction without direct human intervention (Yeoh, 2017; Ng, 2025). In Italy specifically, smart contracts have the potential to push understanding of intent, consent, and cause because they are installed into permissionless spaces that lack central authority to shape how contracts are designed and intentioned. Italy has taken moves to formalize blockchain through the government recognizing timestamping and signatures alongside EU efforts at digital governance and interoperability, but the legal address of when smart contracts fail or where there is third-party manipulation remains tenuous at best (Kamalyan, 2020; Cappai, 2023).

Canada provides a more dynamic yet still indeterminate legal environment. Though smart contracts may be enforceable under the general principles of contract law - where there are the elements of offer, acceptance, and consideration - the absence of a statutory framework defining their legal status puts the interpretation of self-executing smart contracts to the courts and open to interpretation, which can lead to significant inconsistency amongst the courts on whether they would treat self-executing code as an enforceable agreement. This approach becomes an issue when there are legal recourses that would also need to encompass a technical error (Selvanesan & Rodrigo, 2024; Zafar, 2025). It has been noted that Canada has been proactive in encouraging innovation with sandbox environments, while not engaging with key questions, like the legal personality of DAOs, and on whether the terms of a smart contract can be modified retroactively, in the public procurement space (Roy, 2023). In the United States, the enforceability of smart contracts is 'unevenly acknowledged', as some states have laws, like Arizona and Wyoming, that recognize an enforceable smart contract or blockchain statute, but there is still no federal standard. Moreover, courts have been slow to adjudicate smart contracts (and blockchain agreements/methods) due to the inability to enforce through state laws, or case law precedents precedent. As such, smart contracts can create mistrust in their validity for blockchain-based procurement or service contracts because of the finality that comes with the irreversible financial transfer, or service denial, that can come from erroneous enforcement of code. The lack of the clarity - ex ante - surrounding an enforceable smart contract for dispute resolution, on who is liable, and on which jurisdiction (state or not) has an interest in dealing with a dispute limits the use of blockchain in institutional settings with sensitive, or high-stakes, engagements. As a result, a point still remains across all three jurisdictions: legal certainty is a structural precondition to scale up

blockchain applications from experimental pilot programs to systemic infrastructures - goals that existing frameworks are only partially satisfying (Barbereau & Bodó, 2023; Blemus, 2018).

The cross-border aspect of blockchain creates substantial legal friction regarding data sovereignty, jurisdictional reach, and harmonization of international regulatory requirements. More specifically, all three jurisdictions - Italy (EU), Canada, and the U.S. - use legal frameworks that are territorial, while blockchain technology operates in a borderless digital space. This mismatch has generated considerable academic and policy debates about how to regulate a distributed infrastructure that subverts normative jurisdictional boundaries (Zafar, 2025; Herian, 2020). The EU's GDPR has a broadly defined extraterritorial reach, therefore any blockchain network that processes domestic EU residents' personal data must comply with the EU's data protection principles even though the location of the blockchain technology is immaterial (Ibáñez et al., 2018). Visual friction is created for those in the U.S. that provide blockchain and cloud services in the EU, particularly post-transatlantic trauma on personal privacy with issues around mass surveillance, surveillance, data localization, and inverse transatlantic agreements such as the EU–U.S. Privacy Shield (Akanfe et al., 2024; Berberich & Steiner, 2016).

As a member of the EU, Italy has embraced this logic of extraterritoriality in its national application of GDPR and has had regulatory engagement with cross-border flows of data. However, due to the decentralized aspects of blockchain, the question of who is identified as a data controller or is legally accountable for data or enforcement jurisdiction is unresolved. This issue is compounded in permissionless networks because it is impossible to identify any one entity or person behind a block whose activities can be articulated as processing personal data (Tatar et al., 2020). Legal scholars argue that such architectures impose an additional need for developing shared responsibility (i.e. accountability) and shared compliance-by-design into and for technical operations that also meet regulatory obligations without compromising the functional value of blockchain (Dutta et al., 2020; Barbereau & Bodó, 2023).

In a similar fashion to the GDPR evolving the domestic regulatory space, the legal landscape in Canada is also changing. Although PIPEDA is not as explicit in extraterritorial application as the GDPR, it does apply to organizations that collect, use, or disclose personal information while engaging in commercial activity of Canadian residents. This means there could be jurisdictional overlaps, particularly because blockchain applications can be on cloud computing infrastructures or as part of a global financial network (Zhuk, 2025; Selvanesan & Rodrigo, 2024). Canadian regulators have started to think about policy reforms to implement data sovereignty and cross-border liability, however this is mostly ad hoc and fragmented between federal and provincial apportionment of jurisdiction (Ng, 2025).

In the U.S., the lack of a federal framework for data protection creates significant asymmetries of compliance across borders. U.S. federal agencies have shown more interest in trade facilitation and fostering technological innovation than in working on harmonization of privacy rules with international partners (Chadaeva, 2024). This leaves the potential of increased legal exposure for

cross-border blockchain deployments involving U.S. actors in relation to GDPR regulated settings or Canadian expectations. There is a growing message in the literature regarding the importance of multilateral engagement and the willingness to develop regulatory compatibility mechanisms to factor these kinds of jurisdictional overlaps into policy deliberation to avoid the siloed jurisdictional and regulatory "legals" existing, which acts to diminish the scalability of blocks (Faria, 2023; Blemus, 2018).

A key factor impacting the consistency and effectiveness of blockchain regulation is the institutional architecture of regulatory governance. Countries and cities develop regulatory inputs as a result of supportive and coordinated regimes. The institutional face that defines and structures actions are important to consider as they shape how the regulatory frameworks can be actualized on practice when dealing with blockchain technologies. In the European Union for instance, coordination does take place at the supranational level by advisory institutions like the European Securities and Markets Authority (ESMA) and the European Data Protection Board (EDPB) to national authorities. Italy can align to this framing as it can create national strategies that hew towards EU directives and it can also decide how national decision-makers implement their interpretation, compliance, enforcement strategy and agreement (Cappai, 2023; Maume & Kesper, 2023) . Italian regulators appear willing to test co-regulatory frameworks or regulatory sandboxes at this stage but are not surprised by the various challenges that still exist around the regulatory burden, compliance burden and legalistic nature of implementing nationally driven processes with existing EU obligations (Kamalyan, 2020).

In Canada, regulatory authority is divided between federal institutions and provincial institutions, which creates a multi-nodal governance structure. For example, at the federal level, Anti-money laundering (AML) compliance is enforced from FINTRAC and securities regulation still remains a regional issue with securities regulators for example Ontario Securities Commission (OSC). The situation is a derailment of hierarchy, which unifies lawmakers, agencies and provincial regulators separating and evaluating multiple data governance and compliance actions, while generating potential policy fragmentation even for blockchain / digital assets which would do not stall provincial boundaries (Ducas & Wilner, 2017; Selvanesan & Rodrigo, 2024). Blockchain will inevitably situate within the data or financial world through the public sector, increasing the demand for oversight and regulation coordination between bodies involved. If a body of institutions exist to supervise the oversight of blockchain, the trouble is the absence of a centre for regulations lacks coordinated policies, have a capacity to delay regulations, and has tendencies to overlapping forms of oversight (Zhuk, 2025; Ng, 2025).

In the United States, the institutional fragmentation is even more diversified. For instance, federal agencies of the SEC, CFTC, FinCEN, and the FTC can claim jurisdiction over individual aspects of blockchain while states continue creating their own rules (e.g., consumer rights frameworks inputting financial licensing and codes of conduct) Yeoh (2017); Chadaeva (2024). There is no legislative mandate to generate an interagency approach, which means a result of regulatory uncertainty, where enforcement actions substitute for any more cohesive policy guidance. As a

result, the U.S. situation creates a fragmented approach to potentially inconsistent enforcement actions where predictability is uncertain or impractical for understanding compliance (in practice) for blockchain designers and enterprises that operate between state boundaries. Legal and regulatory scholars argue that without structural reforms, the jurisdictional regulatory environment in the U.S. will not be sufficiently enabling for innovation and to have any meaningful input into a standard-setting process at the international level (Zafar, 2025; Roy, 2023).

The legal fragmentation and jurisdictional divergence found in Italy, Canada, and the United States have substantial normative implications for the diffusion and systemic adoption of blockchain technologies. There is a consistent concern in the literature that growth in legal uncertainty is eroding legal certainty which is a precursor to trust, both in markets and in public institutions. The uncertainty around the classification of digital assets, the enforceability of smart contracts and compliance across jurisdictions produces legal uncertainties that will inhibit investment, complicate technical development and deter public sector procurement of blockchain-based systems (Ng, 2025; Roy, 2023). Each of the three jurisdictions have linked the disparate enforcement and inconsistent application of rules and overlapping governing mandates to costs of compliance, delays in adoption, and the tendency for developers and institutional users to be risk averse (Zhuk, 2025; Chadaeva, 2024).

The European context provides an example of a normative commitment to innovating while adhering to a structured and transparent legal framework which explains developments like MiCA and the DLT Pilot Regime. Spatially, Italy is part of an EU-level aspiration to advance Europe's position as a global leader in trustworthy digital infrastructure (Maume & Kesper, 2023; Cappai, 2023). Assumptions of compliance with evolving legislation remain but this is in dynamic tension especially in sectors means that a significant challenge remains for innovation and compliance within the sanctioned (decentralization) norms of blockchain, especially where decentralization is in direct conflict with core legal doctrines like authority, accountability and data sovereignty (Berberich & Steiner, 2016; Ibáñez et al., 2018). Legal scholars argue that regulators are unlikely to realize success without dynamic regulatory responses that allow for new technology to force legally calcified regimes to innovate in order to accept experimentation (Faria, 2023; Barbereau & Bodó, 2023).

In Canada, the emphasis on consultation and principles-based regulation indicates a more flexible approach to the legal framework for blockchain even if fragmented and inchoate. The shifting of regulatory burden to market participants by way of principles-based regulation has left sites of normative ambiguity in crucial areas such as public procurement, decentralized governance, and privacy preserving data structures as there are no rules to seek to comply (Selvanesan & Rodrigo, 2024; Ducas & Wilner, 2017). These gaps will constrain the use blockchain where the government has sought to promote transparency projects, and preclude regulatory entities from adopting technological infrastructures compatible with the legal risk management.

In the case of the U.S., it is difficult to argue that the government agencies were wrong to issue enforcement representations given that institutional reliance is on enforcement. In recent years there have been noteworthy enforcement actions from an array of federal agencies but a coherent normative landscape is becoming a concern as regulators are imposing norms on actors that did not exist at the time of conducting business under a different legal framework. Concerns have been raised about undermining a predictable and legitimate jurisdictional, and market-based context that provides regulatory space for actors in emerging sectors such as blockchain and that adopt a reactive stance on an emergent technology, leading to questions of retroactive penalization, forum shopping and overreach (Yeoh, 2017; Zafar, 2025). Without prospective based legislation, and alignment across agencies, the capacity of Blockchain to provide trusted, scalable, and lawful innovation in sensitive environments will be limited.

Despite the presence of differences in regulation and institutional divergence both the literature on comparative emerging technologies and blockchain, have reached significant consensus on the issue of the need to harmonization of blockchain regulation across jurisdictions. As blockchain technologies advance and applications depart from national borders, the ability to permit legal interoperability will ultimately define the functionalities of the platform and purposes for governance and transnational enforcement. In addition, many legal scholars provide evidence that stalks of regulatory diversity are necessary to generate innovation- particularly in the initial phases of the journey, but long-term adoption will require predictable legal environments and mutual recognition of standards, especially in public infrastructure, financial system practices, and public procurement (Blemus, 2018; Faria, 2023). Failing to see movement of convergence creates the possibility of jurisdictional exploitation of regulatory arbitrage by actors as they try to maximize opportunity while concurrently jeopardizing user protections in sectors with significant associated risk.

In the European Union, the combined aspects of GDPR and MiCA present a member-state model of harmonization that other jurisdictions refer to often, and rarely embody in entirety. Italy's position within this level of supranational order is advantageous in terms of legal clarity and international; however, the vast regulatory burden associated with EU-style harmonization can be a disincentive for small or medium enterprises or exploratory blockchain initiatives unless facilitated with institutional support and interpretive leniency (Akanfe et al., 2024; Maume & Kesper, 2023). Additionally, various aspects of GDPR's extraterritorial applicability issues raise jurisdictional sovereignty challenges in U.S.–EU and Canada–EU data flows, especially where compliance requires using entities that do not operate in Europe (Zafar, 2025; Ibáñez et al., 2018).

In Canada, the literature notes both potential opportunity and inertia. Canada has the institutional capacity and legal framework to reconcile EU-style regulatory formalism with U.S. entrepreneurial pragmatism. Still, without a coordinated national vision or expressed and codified blockchain laws, initiatives are likely to remain isolated across provincial level (Selvanesan & Rodrigo, 2024; Zhuk, 2025). Legal scholarship encourages the establishment of interoperable standards, the formation of Common Law Authorities, and participation in international blockchain governance

forums, to foster Canada’s potential role as regulatory intermediary between the two polarized legal models that transects the North Atlantic; the EU and the U.S. (Ng, 2025; Roy, 2023).

The United States maintains the identity of most resistant to harmonization both within and externally. The United States' regulatory stance has favored unilateral or agency-based interpretations over multilateral harmonization, using arguments about competitiveness and jurisdictional independence to justify these measures (Chadaeva, 2024; Yeoh, 2017). This selected regulatory approach has created walls against using multilinguist in developing a transnational legal framework focused on tools to create blockchain-based contracts, enforcement tools, and dispute resolution. Scholars have stated that unless the U.S. begins to become more active in international standards development forums and adopts at least some minimum viable rules on interoperability, future Incidents will only find the U.S. adapting its blockchain-based legal frameworks farther away from other global jurisdictions—both limiting the U.S. influence, and creating friction for planned Programmed Improvements (Herian, 2020; Zafar, 2025).

In terms of the scholarly literature on legal and regulatory approaches towards distributed ledger technology (DLT) in public procurement, we have identified a heterogeneity of analyses that encompass doctrinal, empirical, and policy approaches but with somewhat mismatched approaches and different forms of integration or separation. Doctrinal work, with specific relevance to the Italian or wider European context, emphasizes textualism of valid legislation (Markets in Crypto-Assets Regulation (MiCA), General Data Protection Regulation (GDPR), EU Public Procurement Directives) while articulating relationships between obligations that relate specifically to data processing, digital identities, or procurement transparency. Doctrinal analyses being more advanced in some respects than the evolving positions taken by jurisdictions or the jurisprudence in respect of for example, the CJEU's recent decisions on data portability, privacy-by-design and blockchain immutability reinforces the necessity to acknowledge plausible significant litigation that might conceivably reframe the compliance obligation for new deployment of blockchain in procurement contexts. Without some accommodation for the development of jurisprudence as applicable to doctrinal accounts they will preferred locate in the direction of over-anticipate legal certainty within an unstable interpretive environment.

More mainly policy-oriented literature is dominant within the Canadian context, continuing to focus on Government strategy-documents, white papers, and Innovation roadmaps; providing insight primarily into regulatory intention and identified future opportunities for blockchain especially in relation to initiatives public sector Digital Transformation. There is often very little evaluative weight attached to policy-orientated assessments and at times assumes a straightforward implementation process moves from policy announcement through to operational modification. By not providing context for intergovernmental jurisdictional divisions, and because of the known influence of bureaucratic "path-dependencies' there tends to be quite a lot of "noise" attached to behaviors when it comes to policy impact that requires scrutiny. Additionally, Canadian Federal systems demonstrate significant diversity of procurement regulation by province such that planned, national-level adoption of blockchain by the federal government will often experience

barriers and inefficiencies to even legislative adoption set out by the proposed policy. While acknowledging the institutional complexity present in much of the literature on blockchain reterritorializes the value of policy-oriented analyses.

The U.S. literature encompasses empirical case study examination—often depicting pilot implementations in states such as Delaware, Illinois, or Colorado, and doctrinal discussion of the regulatory environment (including Federal Acquisition Regulation (FAR) provisions, Office of Management and Budget (OMB) guidance, etc.) Although empirical case studies do frame implementation and provide both technical or procedural dimensions of the scope, they rarely position themselves in discussions about administrative law or apportionment of constitutional authority to procure. Similarly, doctrinal studies often address the many normative compliance issues for blockchain regulation, drawing on wider developments in financial or cybersecurity contexts, with a limited range of application and understanding of (more relevant) public procurement examples are the exceptions. In both cases, there is again limited attention to the blasting, reality of evolving U.S. jurisprudence on admissibility of electronic records out of court, the enforceability of smart contracts, or how issues of state-federal preemption also directly speak to the viability of facilitating blockchain based procurement workflows.

An inconsistency across jurisdictions in the existing literature is the limited theorizing of institutional inertia as a regulatory factor. While some works have noted bureaucratic resistance, regulatory capture, or conservative administrative organizational cultures, few have developed an analytical model to consider how these factors systematically affect the trajectory of blockchain adoption, notwithstanding legal permissibility. This has created a frequent misalignment between legal or policy enablers and real-world implementation outcomes, ultimately detracting from the predictive and comparative value of existing studies.

In consideration of these limitations, this dissertation will explicitly categorize each cited source in terms of its orientation to doctrine, empirics, or policy analysis, and deliberately integrate jurisprudence and institutional inertia which are evolving aspects into the comparative analysis, as opposed to being merely elements in a comparison. This triangulated approach would attempt to not only clarify the formal and interpretative dimensions of blockchain that constitute regulation, but also highlight the reasoning in the respective different institutional contexts that provided the enabling conditions for (un, or differently) similar adoption patterns in Italy, Canada and the United States.

Another common limitation in the literature on distributed ledger technology (DLT) governance, is an inclination to regard legal frameworks and regulatory initiatives as a singular blurry layer of analysis. This elision obscures meaningful distinctions in how the public's adoption of blockchain in public procurement is enabled, shaped or restricted. Legal frames comprise formalization in statutes, constitutions, procurement codes or judicial characterizations establishing binding rights, obligations and procedures. In contrast, regulatory actions take the form of fluid policy instruments such as documents, guidelines, regulatory sandboxes, agency technical standards, or

administrative circulars, and are often viewed to be more dynamic and flexible than regulations. The conceptual between these two types of interventions has created analytic clarity issues - understanding differences in jurisdictions with prudent legal frameworks exhibiting slow blockchain uptake and jurisdictions showing more technical legal frameworks that progress through innovative activity and regulatory workarounds.

In Italy and the European Union, anecdotal academic literature on public procurement is doctrinally favoring the use of formal legal documents, such as Codice dei Contratti Pubblici or EU procurement directives that create obligations on public entities in a proximate nature of accountably responsive market transactions or legal conventions, at a high level of abstraction (elaborating contours specific to this study). The formal legal analysis lens often makes off-hand and to its claim sad observations about regulatory actors that enable things, such as Agenzia per l'Italia Digitale (AgID) or ANAT that may observe, looking forward, that technical guidelines or obligations for digital procurement may disrupt or influence blockchain uptake in some way as important non-legal instruments, are instrumental in displacing actor behaviors and practices that may twine obligations in legislative law. Unless disentangled, the orthodoxy is likely to overstate the necessary determinative force of formal legislation, and may not be fully cognizant about what the contribution of policy experimentation.

In scholarly attitudes to account for Canadian public procurement, a similar flattening of layers exists as examples routinely articulate or reference federal open government strategies, digital procurement road mapping, or Treasury Board Secretariat strategies while also including applicable provincial or federal procurement governance frameworks as if these are a reliable legal norm. The previously articulated conflation disregards the reality of Canada's federal interest, where certain statutory obligations can be harmonized by provincial frameworks, while regulatory or sometimes voluntary programs or funded pilot streams are often in practice independent of binding statutory reform. The conflation, where the previous section remarks have pointedly suggested that one ought not make assumptions about provincial differences in blockchain implementation attributable to statutory obligations, speaks to, in the literature and, or observable differences in rates and scope of provincial blockchain experimentation.

In documenting blockchain innovations in public procurement in the U.S., a majority of authors reference procedural adoption prescriptions as federal frameworks such as the Federal Acquisition Regulation (FAR), characterizing them as state level procurement codes, while also subsuming quasi-regulatory instruments labelled policy instruments, innovation grants, Agency pilot authorizations, or executive orders (albeit non-statutory obligations). These descriptions do not attend to the reality that regulatory types of initiative allow for much more agile Agency than legislative change, while still permitting Agencies to experiment with blockchains while there may be no enabling legal codification regarding blockchain solution efficacy. The interpretive absence of clarity in formal legislation around, by way of illustration of smart contracts applicability or enforcement, the admissibility of blockchain based records could discourage the breadth of scaling in a jurisdiction, even in the presence of active regulatory experimentation.

Largely, by failing to appropriately segregate legal and regulatory domains, considerable literature also fails to acknowledge distinct social interactions and escalation of evolving legal landscapes and institutional inertia. In the legal domain laws develop slowly and through judicial meaning, while on the regulatory side the same laws are enacted through bureaucratic policymaking and at the actions of political turnover of the day. It is this distinction that is at the center of the comparative framework that will be used in the dissertation, which will incorporate both legal and regulatory architectures as dimensions that interact with one another and therefore acts as the bridging of valuable explanatory gap related to understanding the leverage of binding legal rules in conjunction with adaptive regulatory strategies and how they shape trajectory of blockchain implementation during anti-corruption in public procurement in Italy, Canada, and the US respectively.

The comparative review of legal and regulatory regimes related to distributed ledger technology (DLT) in public procurement revealed that all three jurisdictions of the EU (as fronted by Italy), Canada, and the US are making incremental, and in some cases progressive, movement towards a further structured form of governance of blockchain, albeit with three distinct forms of progress shaped by specific legal architectures, regulatory traditions, and institutional capacity. It was clear there are considerable similarities in findings across the literature survey across the three jurisdictions in that blockchain was recognized as a means of improving the transparency, traceability, and auditability in their procurement processes. However, whether or not the characteristics related to these technical advantages can actually be entrenched in legally sustainable and operationally feasible reforms to procurement systems depends on the interaction of particular statutory frameworks and regulatory instruments, and critically, whether these domains of governance are considered distinct into accounting audit or procurement process traceability or both.

In the EU, of which Italy is a member, there are various legally binding and actionable provisions (i.e. GDPR and the MiCA Regulation) at the supranational legislative level regarding a considerable degree of legal and regulatory certainty protecting the route towards governance of blockchain and neutrality as respective and leg welfare legislative instruments. Such legislation eliminates ambiguity as to the development step longitude governance as there are credible and harmonized rules or instruments which will lead to conformity and best practices across jurisdictions for cross border procurement governance and management of digital-assets. But as set out in this review, while providing a solid (<-- (not technically true i.e. "solid" legal context is more elastic) degree of clarity surrounding legal compliance it also places legal obligations on compliance that are narrowly defined at the degree of deliberation and contra to primary features of blockchain such as seamless distributed storage and immutable record; and if "the law is a process of steady reconceptualization" therefore the law is dynamic and assumes conditions on the continuum turning it towards legalizable and regulatory compliance. Italian scholarship clear illustrates that these tensions are not only real, but also that they are shaping their system design options and pushing developers into technical workarounds such as off-chain storage, hashed

pointers, and pseudonymization to fulfill transparency when they are constrained by a law governed by privacy. As many authors have noted, any such solutions that solve such problems have to be consistent and aligned with the current corpus of CJEU jurisprudence on procurement law and collaborative regulations nuances, perhaps demonstrating again the interconnected nature of legal and regulatory governance.

Canada is positioned in between a principles-based regime (notably the Personal Information Protection and Electronic Documents Act PIPEDA) and regulatory jurisdictional divisions. While a federated jurisdictional structure allows for innovation through regulatory sandboxes, pilot programs, and flexible compliance regimes, the regulatory scheme is fragmented and results in uptake that is variable across provinces. The literature suggests an enduring gap between national policy and subnational implementation of initiatives, indicative of institutional inertia, and intergovernmental coordination. Without an articulated set of national standards for blockchain in procurement, potential Canadian projects will remain isolated pilots instead of functioning distinct parts of a national infrastructure.

The United States exemplifies the most fractured and enforcement-based model. In the United States, blockchain-related procurement projects are in a substantial governance environment of federal statutes, specific state laws, unique agency rules, and competing jurisdictional claims by the SEC, CFTC, FinCEN, etc. This pluralism enables a range of pilots in procurement and provides the chance for rapid experimentation. However, the resulting legal uncertainty specific to smart contract enforceability, blockchain record admissibility, and inconsistent, sometimes different, state laws on privacy is immense. The literature points a connection between legal uncertainty and vendor compliance costs, vendor risk-adverse behaviour, and no legal framework to support systematic adoption in public procurement.

A critical contribution made in comparative literature has been to analyze the important distinction between binding, enforceable statutory regimes (statutes, public procurement codes, judicial pronouncements) and more adaptable regulatory regimes (regulatory guidelines, technical standards, sandboxes). Where these two forms of regime(s) have been conflated, as they are in much of the existing literature, it is challenging to explain why jurisdictions with relatively permissive legal contexts have relatively slower adoption practices, or alternatively, why jurisdictions with more restrictive statutory regimes have some fast-paced regulatory experimentation. Codice dei Contratti Pubblici - Italy, procurement statutes - Canada, and the Federal Acquisition Regulation (FAR) - US, all establish legal benignity, but the speed of adoption can equally be influenced by the maneuverability of the enforcement agency or jurisdiction's, efficiency of regulatory bodies (for example, AgID and ANAC - Italy, provincial commissions in Canada, state innovation offices in - US).

Institutional inertia also represents under-theorized characteristics. Notwithstanding the enabling legal regime or proactive regulatory regime, the administrative culture, the capacity of a procurement office, the lock-in of vendors, and typical bureaucratic resistance have the potential

to delay or obstruct blockchain adoption across procurement systems. Regulatory interventions undertaken with a target-specific focus such as Italy's work with the EU DLT Pilot regime, and the sandbox framework made available in the provinces in Canada - could act as a catalyst to accelerate adoption as long as it is underpinned with sufficient institutional capacity and political will. In addition, the US demonstrates how, without inter-agency collaboration, these efforts can be also siloed in approach, producing little to no transferable lessons or policy.

Across the three jurisdictions examined, the most viable pathway revealed in the literature has been found in the conscious engagement of legal certainty and regulatory flexibility. The legal framework must be clear enough to confer enforceable rights and duties onto parties engaged in blockchain-based procurement, while the regulation must be sufficiently flexible to allow regulators to adapt their oversight to changing technical and operational realities. The comprehensive coordination and engagement of legislators, regulators, technologists, and public procurement operators, as well as appropriate means for comparative policy learning that acknowledge the realities of jurisdictions will need to be maintained.

In conclusion, while the technical capacities of blockchain to address corruption risks in public procurement has been well-established, it remains dependent on the integration of effective and accountable governance processes at least partly derived from legal certainty, clarity and coordination. Italy’s EU harmonization of laws, Canada’s principled based federalism and, the United States’ fragmented pluralism all present different opportunities and trade-offs. A comparative perspective suggests that the effective implementation of blockchain in public procurement is less a matter of expounding blockchain-favorable rhetoric in policy documents, but rather the extent to which statutory declarations, regulatory apparatus and institutional practices are organized toward the same outcome. The analytical framework presented in this dissertation will help to address this organization of effort with respect to the distinction between the formal authority of law and the more flexible regulatory authority, both being situated within the political–institutional context that will ultimately determine the pathway to integrated blockchain assembled public procurement systems.

Synthesis. The comparative analysis indicates that some DLT designs can only be realized with jurisdictionally specific safeguards. In the EU/Italy context, a permissioned, consortium ledger as either an integrity layer or audit layer—interoperable with PAD/BDNCP—becomes plausible only where personal data is minimized, with any personal data kept OFF-chain, any ON-chain entries only limited to cryptographic commitments without friction from personal data, and qualified trust services (eIDAS) used for signatures and seals. Additionally, any smart-contract logic must include interpretability, access controls and event-logging congruent with the Data Act, and records retention and publication/transmission must emanate from a repository that is authoritative and inclusive of the records retention schedule and used ANAC conformant interfaces. In the Canada context, the construction of a CanadaBuys-adjacent integrity ledger is not feasible without using UECA compliant e-signature workflows, PIPEDA aligned purpose and retention rules in practice, appropriate identity assurance consistent with PCTF/GCKey stack, and evidence bundles

exportable sufficiently to comply with the Canada Evidence Act (including system reliability, chain-of-custody, time-stamping). Differences in provincial and federal landscapes require a policy understanding of time-limited retention rules as a centralized measure for standardizing retention "clocks" and routing accordingly. In the U.S. context, the construction of a permissioned layer that has agency scope and leverages tamper-evident commitments creating links between SAM.gov/FAR processes can only be predicated on identity proofing that exists at NIST SP 800-63 levels (mixing identity proofing and identity assurance such as IAL2 via Login.gov), signature attestations grounded in an ESIGN/UETA taxonomy, retention schedules in compliance with OMB/NARA and FOIA compliance including redaction/export, and a pathway for evidentiary certifications of real-world information that would be suitable enough under FRE 901/902(13)/803(6).

Operational blueprint. Across the jurisdictions considered, the defensible leverage is a three-layered architecture; (1) identity and trust-services layer for enrollment, authentication and qualified signatures/seals (government eID or accredited TSPs); (2) record and evidence layer with authoritative OFF-chain stores, OFF-chain retention/enforcement, legal-publication adapters, and the ON-chain INTEGRITY proofs; and (3) contract-automation layer that contains smart-contracts to narrow, audited and reviewable routines which can "kill"-switch and role-based access. The legally durable three-layer architecture is fundamentally supported by "packaged" leadership and governance structures (independent oversight node, change-management charter, code escrow/exit plan), legal structures (terms of ledger evidence, portability terms, DPIA/PIA artefacts), technical and systems structures (fine-grained access control, event logging, schema versioning, deterministic audit exports), and assurance structures (identity and controls-testing, conformity assessment, disaster-recovery proofs). With this framing, §2.4 yields useful concrete propositions for subsequent comparative chapters: for example, the EU/Italy prerequisites for using its trust-service and smart contract features should at a minimum reduce compliance risk to milestones-payment automation relative to the US, given the compliance issues of FOIA/NARA constraints and state privacy empirics which push conventional logic more OFF-chain; further, Canada's provinces' alignment around PCTF/UECAS supports similar feasibility provided that specific description of evidence packaging, retention governance and data portable governance are specified ex-ante.

3.Conceptual Framework, Research Methodology and Conclusion, Contributions, and Recommendations

3.1.1 Governance and Institutional Theory

Understanding the role of blockchain in public procurement system reform would require a solid theoretical understanding of governance and institutional change. Governance theory, and specifically its application to the modernization of the public sector, allows us to theorize about how governance arrangements (e.g., power relations, decision-making processes, accountability mechanisms) can be altered by new technologies - like blockchain - within a procurement system. Institutional theory provides insight by explaining the rules (formal or informal), organizational routines, and norms that will mediate how technological innovations are adopted or incorporated into procurement systems. Together, governance theory and institutional theory will provide a multidimensional understanding of blockchain reforms in public procurement, and position blockchain not solely as a technical system, but as an institutionalized governance instrument.

I. Governance as a Context of Multi-Actor, Multi-Level Property

Current governance studies literature affirms the devolution of power and authority among multiple actors, levels of governance and mechanisms of control in governance networks. Traditional bureaucratic command and control measures are being replaced by networked, collaborative governance based in creative partnerships with public authorities, private contractors, civil society actors, international organizations and most recently, technological systems (Kooiman, 2003; Rhodes, 2007). Public procurement is paradigmatically governance—characterized by legal-administered agreements, budget considerations and competitive market conditions, decision-making based factors such as political priorities, technical efficiency, and procedural legitimacy. Blockchain technology, and specifically decentralizing and automatized ability of blockchain technology, opens ways of governance and includes rule enforcement, transparency and auditability within the architecture of the system. That novel technology has transformed control from human-mediated governance to technology-mediated governance initiatives and has raised new concerns related to legitimacy, control, and adaptation (Peters, 2012).

Blockchain exists as an actor and tool in governance networks, as the enactment of rules moves from discretion to set using a computer algorithm. Smart contracts, automatically enforce conditions; automated verification of identification conditions and irrevocable audit trails can change past relationships of accountability, created in discretion and adherence to a social architecture, into different accountability functions through governance by algorithmic systems. The challenge is whether the changes in the distribution demonstrate improvements while maintaining the foundations of governance on which it rests as transparency, inclusion, and procedural legitimacy (Sørensen & Torfing, 2007). Therefore, the discussion of blockchain and public procurement governance must also be theorized in terms of institutional re-shaping instead of simply considering technical reform.

II. Theoretical Consideration of Institutional Theory and the Path Dependence Logic

Institutional theory is an excellent theoretical perspective to capture both the inertia and change processes that inform public procurement processes. Institutions, as rules, norms and organizational structures, that remain stable long-term (North, 1990), impose limitations and enable adoption of new technologies and constrained opportunities. Procurement processes use statutory codes, bureaucratic routines, and professional cultures, that generate strong path dependency, creating mechanisms of resistance to change. Innovations that use blockchain, which is based on decentralizing the governance process, automate the contract process and provide transparency that counters the institutional logics of official recourse and enforcement procedures, will always depend on whether the elements of the innovations cohere with institutional structures, or alternatively, together reshape existing institutions.

The concept of institutional change is generally not a singular event, and as Mahoney and Thelen (2010) have indicated institutional change proceeds through inscriptive and gradual frames that suggest layering (including new/additional component), displacement (substituting one rule with another rule) or, conversion (old rule/structure adapted to new purpose). Each of these three framing ideas are relevant in the discussion of blockchain and public procurement governance literature. For example, public procurement e-procurement platforms, may layer a blockchain audit trail on an existing proprietary database, or existing statute, that alters no legislative arrangements; smart contracts may displace an old discretionary space by hardcoding the terms of payment, which are arguably still captured in unintelligible legislative documents; or, blockchain arrangements may be deemed legitimacy-promoting processes and provide anti-corruption security that is connected to stable forms within varied statutory contexts, without changing any existing legislative processes.

Thus, as you develop the adoption process of blockchain, frameworks of institutional property will be salient features in the boundaries of the analysis through an institutional lens: organization capabilities, regulatory traditions, public procurement practice, and how it exists in connection to the wider governance regime. Theoretical logics of institutions are premised on stability, legality and accountability, and are both present, and necessary for, agents of change to emerge in procurement, irrespective of the agenda—ministries or intergovernmental task committees attempting to find new/old ways of innovating.

III. Institutional Isomorphism and the Role of Legitimacy

Institutional theory also can explain the ways that public sector organizations converge around similar technological solutions, this convergence is driven by isomorphic pressures which cause organizations to establish similar structures, technologies, or practices in order to gain legitimacy (DiMaggio & Powell, 1983). In the case of blockchain, the coercive aspect of isomorphism would be caused by regulatory pressures such as the EU's digital directives, or WTO procurement standards. The mimetic aspect of isomorphism would be presented by organizations trying to emulate organizations that they view as the best in the industry, such as Estonia in this case in blockchain-based registries. The normative aspect of isomorphism would be through the

professional networks of the public sector that advocated for a shift to digital transparency as an ideal for procurement.

However, isomorphic adoption could lead to superficial reforms if the organization is striving for legitimacy through symbolic compliance instead of substantive change. This is often seen in pilot or demonstration use of blockchain systems, rather than a deep integration into the procurement workflows to implement structural changes, leading to what has been referred to as "innovation theater" (Mergel, 2016). To ensure a successful reform process, the proposed isomorphic use of blockchain should be aligned with the existing institutional goals of the organization, seek to build internal capacity, and offer evidence of providing meaningful value when enhancing integrity, efficiency and trust in procurement processes.

While institutional inertia is clearly a barrier to blockchain adoption; it is important to also extend our discussion into more detailed accounts of specific actor challenge categories in reluctance to use blockchain and its corresponding barriers to entry into the public procurement systems. One of the key challenges to blockchain usage would be the resistance to change from existing and entrenched procurement actors, including procurement officers, politicians, and contractors; who may view blockchain implementation as a threat to their power, discretion, and financial interests. As an example, public procurement officials may dismiss blockchain systems that automate contract validation procedures or payment release due to reduced human autonomy (Sørensen & Torfing, 2007). Similarly, contractors may feel exposed due to the increased transparency of blockchain which could create increased competition and decreased profit margin.

Jurisdictional fragmentation with respect to emergent technologies in federal systems (like the U.S. and Canada) also poses obstacles, as levels of government increasingly differ regarding blockchain adoption (GAO, 2023). Resistance from incumbent vendors in Italy who enjoy monopolistic control over procurement systems can complicate blockchain adoption. Resistance can also be compounded by lower levels of digital literacy in certain regional contexts which complicates situational adoption of emergent technologies such as blockchain into existing procurement procedures.

As a result, overcoming these obstacles will and must be gradual and inclusive, meaning that stakeholder engagement, capacity-building, and policy alignment must be considered. Without these considerations, blockchain use in procurement will suffer from the same pitfalls that many public sectors pilot projects experience, i.e., because they are technically sophisticated projects with no significant institutional changes prior to or after implementation (Bovaird & Löffler, 2016).

IV. Governance Capacity and Institutional Resilience

A final consideration of the adoption of blockchain technology is governance capacity— or the agency of an organization to design and implement policies and also the ability to accommodate policy and technology to situations that are complex and transitional. Blockchain presents new

technical, legal, and ethical questions for decision-makers, so this critical reactivity includes things like experimenting with regulation (e.g., sandboxes), inter-agency collaboration, and public–private partnerships. These new reactions and approvals are not equally available across jurisdictions. For instance, Canada has a centralized digital innovation unit that is open to this experimentation and innovation, while Italy's procurement bureaucracy is extremely fragmented and formalistic. The decentralized innovation landscape might allow U.S. organizations to experiment locally though this arguably also exposes the U.S. to risks of fragmentation without standards (GAO, 2023).

Governance and institutional theory make it clear we view blockchain not as a neutral technology, but as a contested reform that has to be viewed from its institutional histories, organizational politics, and governance architectures. Without engaging with these considerations, we cannot adequately determine whether or not blockchain will compound extant procurement pathologies or shift them to more accountable, transparent, and equitable systems.

3.1.2 Legal Pluralism and Technological Regulation

The viability of the introduction of blockchain technologies to public procurement systems aimed at regulating corruption must be viewed through the lenses of legal pluralism and technological regulation. These lenses provide a fuller proposition of how blockchain relates to codified rules, and with other norms, regulatory logics, and institutional cultures and interpretive traditions. Berman (2007) and Teubner (1997) define legal pluralism as the existence of multiple or distinct normative and regulatory orders within a single polity or jurisdiction. This definition reveals that law is not merely a single constraint on innovation, but rather a multitude of culturally-based discourses that overlap concepts. Public Services and Procurement Canada (PSPC) in Canada has disclosed its intention to execute initiatives that are predicated on the investigation of blockchain technology in digital services contracts (Government of Canada, 2023).Additionally, the province of Vermont has also officially recognized the legal status of blockchain documentation in public sector transactions, while permitting some extent of experimentation concerning the use of blockchain technology for government contracts (Marinos, 2020).

In the U.S., pilot programs in the General Services Administration (GSA) are exploring blockchain technology for federal procurement, looking to create transparency and minimize potential manipulation and operational risk in supply chains (GAO, 2023). Blockchain technology is also being tested in defense procurement with smart contracts that have been developed to support the automation of invoice verification and supplier compliance (Werbach & Cornell, 2017).

The above instances demonstrate that blockchain technology is an active move away from theoretical and being employed by a range of jurisdictions to promote increased transparency and accountability, with the potential to mitigate corruption.

I. Blockchain as a Regulatory Artifact: Disrupting the Legal Hierarchy

Blockchain is a regulatory artifact, thus when we consider regulation, it is not confined to data recordation, but ability to condition behavior and enforce norms. In trying to achieve the above, legal systems expect institutions to interpret rules, validate norms, and subsequently adjudicate disputes ex post facto. Blockchain enables ex ante enforcement; meaning, compliance is encoded through smart contracts, consensus protocols, and immutability rendering the contribution of legal actors unnecessary. This paradigm shift raises fundamental challenges surrounding the law relating to administrative governance and procurement standards, particularly in jurisdictions with a civil law orientation such as Italy, where formalism, codified legislation and stratified legal legitimacy play prominent roles.

The notion that “code is law” (Lessig, 2006) directly demonstrates this dichotomy. On one side, smart contract espouse greater transparency, efficiencies, and resistance to corruption in procurement processes by eliminating the discretionary bottlenecks or points of human intervention. On the other side, such determinism is not without its vacillations, as contracts often cannot fully infer inevitable scenarios, and algorithmic logic cannot always replace legal reasoning or judicious proportions of equity and procedural fairness (refer to Werbach & Cornell, 2017). This means the application of blockchain technology in procurement, must navigate the rigid logics of computational logic, whilst also capturing the interpretive elasticities of legal norms and practice cases, especially because the capability of contracts to defer to a traditional logic-based structure predominantly reflects circumscribed and relatively narrow in-scale formats of incremental negotiation, resolution of disputes and to a certain extent the ability to bring forth exceptional categories that trace legality with large scale procedural limitations.

One of the biggest hurdles to blockchain adoption surrounds legal frameworks that relate to the immutability of blockchain records, especially with respect to privacy laws, as is the case with the General Data Protection Regulation (GDPR) in the European Union. The GDPR defines "right to be forgotten", as it relates to the ability of a person to request that an organization deletes all personal information, which, is often impeded by the immutable nature of blockchain technology that means once data is written on a blockchain, this cannot be deleted without compromising the integrity of the entire ledger (Finck, 2019). This aspect of law is also significant for public procurement where contacts routinely include personal data such as when records are made public. The EU has not created a definitive resolution to this dilemma, but the use of regulatory sandboxes is permissible in order to explore privacy-protecting blockchain approaches, such as certain zero-knowledge proofs, which could allow data validation without exposing all of the data (Zetzsche et al., 2017).

In the United States context, the California Consumer Privacy Act (CCPA) poses a similar dilemma, whereby it is asserted individuals have a right to request deletion of their personal information, which could be at odds with blockchain data's immutability (Bradshaw et al., 2019). One fix compares to the principle of off-chain storage of sensitive data, where only hashes of the data are placed on the blockchain; this means that organizations could fulfill privacy obligations while satisfying the audit trail provided by blockchain (Corrales et al., 2019).

These legal challenges stress the necessity that we design blockchain systems not only to meet blockchain's potential for transparency and accountability, but that they also fluently manage one's ability to fulfil the rights of privacy that underlie legal obligations.

This issue surrounding law, the law of the procurement process is especially acute; realizing that any legal obligations themselves are conditioned by very real administrative requirements such as equal treatment, transparency, competition and due process. Automating decision making in complex governance experiences can lead to 'relaxed' forms of constitutionalism when agency values are either circumvented or arguably diminished by automated blockchain practices-feeding a professionalized notion of engineering when public bodies interact with contractors, operating in private law relationships under very unbalanced structures of power- or when there are through various dispute processes, required legally focused or technically-based illegitimacy within the legitimacy of implementing automated procedures in public organizations. Realistically, these types of models present all the qualities of rule formalism devoid of any normative depth, especially when released publicly without legal safeguards, procedural defaults or contingencies.

II. Jurisdictional Pluralism and Regulatory Fragmentation

Another layer of complexity stems from the cross-jurisdictional nature of procurement law. In the European Union, Italian public procurement is governed not only by national law (notably, the Codice dei Contratti Pubblici) but also directly by supranational directives (notably Directive 2014/24/EU), creating a multi-level legal order. Any procurement infrastructure built on blockchain must embrace interoperability with both types of legal systems. For example, if a smart contract is being used to automate selection of suppliers or payment to suppliers based on prescribed conditions, the relevant procurement law will still apply (e.g., EU rules on transparency, right to remedy, fair competition). A blockchain cannot be relied upon to create opacity of procedural or substantive nature for legitimate actions, nor can procedure be simply displaced by algorithms and immutably code that risks standardizing discrimination (Hildebrandt, 2015; Finck, 2019).

In Canada, federal, provincial and municipal procurement systems articulate with each other but operate within three distinct legal frameworks. Federal procurement by the Government of Canada, which is subject to Public Services and Procurement Canada (PSPC), preceded concurrent systems established and maintained by provincial governments in the same country which rely on supply arrangement systems. Adoption of blockchain technology may need to accommodate procedural interoperability due to overlapping responsibilities of distinct administrative authorities. Even if intended for domestic use, the wider context for institutional procurement in Canada is multilayered because Canada is party to several treaties (e.g., CETA, CPTPP, WTO GPA) which require Canada to abide by standards for fair procurement processes and other rules related to data and access to markets. A blockchain-based procurement system cannot inadvertently breach treaty obligations, for instance by illicitly embedding a discriminatory selection logic or compromising availability of assurance in different jurisdictions.

In part, the pluralism of regulations in the United States is analogous to the lock-step jurisdictional complexity of the CETA and CPTPP frameworks described above, with the distinction being rooted in the federalist role and structure of the Constitution of the United States. Federal procurement is subject to the Federal Acquisition Regulation (FAR), however, as has been noted, each State is entitled to structure its own rules for procurement including any designs for digital innovation. This results in both flexibility and fragmentation: while individual agencies (e.g., the Department of Defense or General Services Administration) can pilot blockchain projects, the decentralized nature of regulations means that without a national interoperability standard, legality can become complex, and therefore, fragmentation makes the United States a good case for examining how blockchain can be localized, modular, and reconceived under federated procurement regimes.

When taken together, these jurisdictional comparisons show that the anti-corruption promise of blockchain is not a technical feature but rather a context-centric, institutional outcome. Just as what might work in Estonia or South Korea may not be able to happen in Italy or Louisiana, (due to legal, administrative, and cultural variations) so too, legal pluralism should not be viewed as a limitation to be abolished, but instead, it should be embraced as an empirical and theoretically variable within any comparative study of blockchain-based procurement reform.

III. The Rise of Embedded Normativity and Technological Regulation

Legal pluralism is further complicated by the emergence of technological regulation; a paradigm of regulation, where legal rules now appear to be built-in or embedded as a part of the digital system's architecture (Brownsword & Goodwin, 2012). Blockchain is one such example of this shift, as it is now able to encode the various rules surrounding procurement norms (e.g., time-stamped submissions, who the supplier is, payment triggers) into the logic of the system in a way that actually minimizes third-party discretion, collusion, or encountering corruption. However, whilst this "legislation by design" is introducing a form of embedding normativity, it is also introducing both epistemic opacity and normative rigidity: the more the law is encoded into code, the opaquer it becomes to the actioning of non-technical actors, and the more fixed (meaning no consideration to multifaceted layers of regulation could be taken) the operationalization of that code becomes. "Hardwiring governance" can raise several risks, including legal irrevocability, unequal access to system inputs (e.g., if smaller suppliers do not have the technical capacity to interact with the blockchain), and diminishing legal oversight. Established processes of administrative law, such as public hearings, consultations with stakeholders and appeals if decisions are automated and flow through the governance system without transparency for procedural fairness, may be undermined or ignored altogether.

This is not simply conjecture. Consider evidence from early blockchain pilots in procurement, for example in Colombia and Chile, which demonstrate that technical innovation does not guarantee institutional convergence, but rather result in parallel systems of governance where automated

decisions sit alongside non-reformed bureaucracies, and the risk of confusion and inconsistency surrounding legality and legality (Kshetri 2023).

Legal sovereignty considerations and identity governance are also significant in blockchain procurement, as who owns the node infrastructure? Who approves transactions? Who is permitted to access the ledger? In cross-border projects, the respective impacts of privacy laws (e.g., GDPR (EU) vs. CCPA (US)), data localization rules and mandatory audits raise additional challenges. A blockchain system that keeps records of procurement logs on decentralized servers may violate respective national data protection laws without legal protections, such as zero-knowledge proofs, permissioned ledgers or legally binding interoperability frameworks.

IV. Regulatory Innovation and Adaptive Legal Ecosystems

Given these tensions, multiple jurisdictions are trialing regulatory sand boxes, soft laws, and pilot regimes, as opposed to complete legislative reform, to investigate emerging blockchain applications. These models herald the transition from “command-and-control” regulation to adaptive legal ecosystems where the legal accommodations of technology are guided by experimentation, feedback and co-regulation (Zetzsche et al., 2017). Blockchain records and smart contracts have been formally recognized as legal in the U.S. states of Arizona and Vermont. The Canadian government's Digital Charter also suggests a regulatory framework around technologies enhancing public trust in the context of Canadian public services. It could be said that Italy is more conservative, but Italy is involved with EU funded projects such as the European Blockchain Services Infrastructure (EBSI), which suggests some greater interest in legal harmonization and technological uptake.

That said, the fact regulatory sandboxes are utilized should not excuse the demand for normative clarity. Temporary exemptions and pilot waivers may not replace clear rules around contractual liability, avenues for dispute resolution, due process, and data governance. Hence, the legal accommodation of blockchain must move beyond experimentation to co-evolution, or a stage in development where technological affordances contribute to legal design, and users are engaged in legal and normative considerations. As such, this approach will need to maintain the foundation of key procurement principles—fairness, competition, and transparency—even as it embarks upon new paths to innovation and decentralization.

Towards a Hybrid Legal-Tech Governance Model

The focus on the intersection of legal pluralism and blockchain technology highlights dramatic changes to the distribution of regulatory authority in public procurement. Blockchain creates new digital pathways—the digital presence transforms—not only how rules are enforced, but interaction among actors and the legitimacy described as prior (in the sense of natural law or legitimacy of the public sector) to the emerging digital presence. Yet any success embraces and aligns with polycentric legal orders, and preserves procedural rights and legal remedies.

Where legal pluralism may inhibit, this dissertation approaches legal pluralism as both an essential state of being with respect to governance of blockchain in procurement. Effective anti-corruption outcomes follow only when blockchain understands that it is not a blanket technical fix but a set of contingent institutional intervention(s), reflective of the layered legal architectures comprising Italy, Canada and the U.S. A comparative study based in circumstance is needed to theorize not whether blockchain can address procurement corruption, but the conditions of legitimacy and efficacy can only be met under certain institutional and legal realizations.

3.1.3 Public Sector Innovation and Digital Trust Models

Reconfiguring Public Innovation via Digital Trust

Public procurement systems are currently undergoing a transformation through innovation and, at the same time, restoring trust. These systems have been rife with procedural opacity, discretionary corruption, and inefficiency leading to public mistrust and hobbled service delivery. In this environment, blockchain enters the scene as more than a digital medium, but rather as an artifact in the apparent movement for the public sector to develop a technologically mediated layer of trust. This subsection will explore the conceptual linkages between blockchain implementation, public innovation and digital trust framed within research on institutional change, technology and digital government, and behavioral models of trust.

Public innovation in the public sector has typically been engaged by bounded experimentation within vertical bureaucratic administration. However, blockchain can grip public innovation in a surprise way by automating accountability structures, share new decentralized platforms for creating new sources of trust that shift from the institutional field to a computational ecology (Mergel, 2016; Kettunen & Kallio, 2020). Additionally, blockchain technology is not value neutral and carries instrumental value by promising rationale of transparency, fairness and auditability. The ability for blockchain to fulfill its promises depends on its interaction with existing trust structures in dynamics in the public sector - including legal social norms, administrative procedures, perceptions of trustworthy dealings, digital literacy and institutional credibility.

I. Public Sector Innovation: From Process Digitalization to Structural Disruption

As observed, public sector innovation has been solely focused on process and workflow improvements; digitizing existing processes and workflows, increasing service delivery efficiency and reducing administrative burden are key objectives for the public sector. Spatially, e-procurement platforms provide a good example of the move to improved workflow, by switching from paper-based bidding to online bidding portals, but do not alter existing power structures of accountability. Blockchain represents a qualitatively new technology; it disrupts the authority mythos of public institutions (the prescriptive rules of verification), automates compliance, and allows records to be tamper-proof from its design (Janssen et al., 2020). In other words, the structural change can be understood as disruptive public innovation, where innovation is

understood to reshape existing dominant logics of institutional norms, roles of actors, and flow of information (Osborne & Brown, 2011). Societal examples of technology producing disruptive innovation are prevalent, notably in the recent example of public procurement. The benefits of smart contracts as an element of public procurement are exactly in the removal of decision-making capabilities by contract managers, and the legal authority to comply with pre-coded logic. This decreases the likelihood of collusion and manipulation but opens new dilemmas around monitoring, describability, and exceptions. More importantly, while the innovation has a distinct technological (as opposed to social) origin, it alters governance; blockchain creates accountability regimes (e.g. transparency by algorithm); alters risk [profiles]; (e.g., from human-judgement error, to code failure); and the emergence of new knowledge, skills, and capabilities needed from public agencies to regulate and operate (Vogl et al., 2020).

In this sense, blockchain innovation in public procurement is an extreme example of a socio-technical transition, but addressing how to build readiness from a readiness-state, capability, policy coherence, and cultural readiness in such a way to conceptualize, develop and legitimize a expertise of (human) capability to audit a system, develop smart contracts, work with other policies and sectors, and understand our own digital ethics related to work. If public workers do not have these capabilities, the blockchain systems poses a significant risk of being 'pilot projects' that are merely sophisticated technology.

II. Digital Trust: Blockchain and the Reconstitution of Public Legitimacy

In public procurement, trust is a multi-dimensional construct consisting of interpersonal interactions or procedural trust (eagerness to believe the procurement processes were undertaken fairly and with transparency), institutional trust (the belief that organizations have the capacity to act responsibly and competently), and technological trust (the willingness to believe a digital technologies is safe and reliable).Corruption corrupts all three levels by inducing perceptions of favoritism, inefficiency, and lack of transparency. Traditionally, efforts to restore trust consisted of new regulatory frameworks, auditing, and external oversight regimes. Blockchain presents a different logic, which is to create trust by design. This refers to the notion that systemic credentials can be built into infrastructure with proper transparency, automation, and decentralization (Zyskind et al., 2015; Atzori, 2015). At the basis of this logic is verifiability without trusting institutional intermediaries. A public tender on a blockchain is timestamped, immutable, and visible to relevant actors. This challenges the information asymmetry used to carry out corrupt behaviors. Smart contracts enforce milestones in procurement without granting the discretion necessary for corrupt behavior, and decentralized audit trails provide non-repudiable forms of traceability. These arguments stand for new computational trust based on protocols and guarantees made possible by cryptography.

That said, blockchain does not purge institutional trust. It instead redistributes institutional trust. Trust is both distributed and dependent: not just in the technology itself, but in the actors in the ecosystem who maintain, seek consensus, and interpret the blockchain system. Therefore, public

trust relies on how the system is governed, accessibility and remediation. For instance, if a smart contract executes in error because of a misconfigured rule, what happens next? And who is responsible?The advent of blockchain does present new types of hybrid accountabilities and failures - a combination of legal liability, administrative accountability, and technical failure (Weber et al., 2022). In addition, citizens' trust in digital infrastructure is also shaped by socio-technical narratives. The technology can be all the more secure, yet it has to be perceived as safe by the public. This includes commitment to transparency, digital literacy, and citizen engagement. Without engaging in systems-thinking, blockchain is yet another machine that is going to displace something already existing - not that we are trusting. The challenge in part has to do with the fact that in jurisdictions where low institutional confidence has historically existed, for example use case jurisdiction Italy - blockchain is an easy target for skepticism. Skepticism that stems from dead, dried legacy reform that went wrong with all kinds of accounting and audit paralyses (Galli et al., 2023).

III. Enabling conditions for Block-Chain Trust ecosystem

For the successful institutionalization of the use of blockchain in public procurement, we will need enabling conditions - and by enabling conditions we mean technical, organizational and normative. Firstly, in order for WMDS to support decentralized ledger technologies - minimal digital infrastructure will need to support such features as: verifiable identities, interoperability of data standards, and connectivity. Without these all that blockchain does is enhance the digital divide. Secondly, organizational preparedness - public procurement must confirm understanding of blockchain, revamp procurement workflows to integrate, and re-think how the organization will deploy resource and develop a governance framework to manage distributed verification practices and automated smart contracts sponsors; that may include requiring, or re- defining procurement officer roles to assess objective mapped standards, and developing blockchain ethics panels, or formalized partnerships with civic tech organizations and auditors.Thirdly, and most importantly the ecosystem must invest in normative alignment - that is ensuring that the blockchain innovation aligns with the legal, ethical, and cultural expectations of the societies in which they are situated. We can no longer simply automate procedures, but will be required to embed values which advance public values - implies inclusivity, and due process, proportionality; and develop balance disclosing information (i.e. identity of bidders) and accountability necessary to engage in the automated or machine support decision - while retaining a human way of legal recourse. Therefore, trust is not produced as a technical outcome of automation or systems design - but is co-produced by sociotechnical alignment.

This alignment is not static - transaction of public procurement is, and experiences uncertainty, and the technology block-chain also experiences uncertainty throughout lifecycle development. Institutional logics themselves will need to change along with how organizations monitor and mitigate risks associated with public procurement, through re-imagined institutions technologies

will need to be launch and realize new corruption risks and legal response developments. Countries such as claws Estonia, have successfully changed policies to develop digital infrastructures such as population registry, and or digital identity systems. Estonia's development shows the importance of scoping an institutionally strategic sequence of implementation - publicly scoping small, principled activity and successfully achieving a couple of successful use cases is a huge but very meaningful first signal to beginning the role process that has huge complexities to the institutions that are more significant implies (i.e. public procurement) than the small use cased experimented with.

innovation as a strategy to build trust

Public procurement reform is ultimately a legitimacy-enhancement project. Blockchain is an opportunity to be thoughtful in embedding a method for re-building institutional trust as an embodiment of layering transparency, reducing appropriate discretion, and facilitating accountability in real-time through the right hardware capacity for it. But it has to become more than an institutionalized practice of software capacity - hardware capacity can easily become a software capacity and reference lost value. Blockchain is not a one-off in digital design, that's first characterized as a technical innovation plan - but integrated into the suite of digital strategies with similar interests for users - legal protection round liberal systems, participatory governance, and value-based system. This comparative lens of the communications - task in this dissertation - rests on the complications of three (3) democracy-based institutional reform opportunities to examine how different systems of innovation, legal cultures, and trust environments affects plans projects to roll out should feel by the type of institutions in repair (i.e. across distinct jurisdictions); we describe blockchain as a tool but signifying its potential as a multi-layered architecture (in this case for trust) conversely clarifies how anti-corruption and governance innovation intersect towards a better democratic world order.

3.2.1 Decentralization, Transparency, and Auditability as Anti-Corruption Enablers

The relevance of blockchain to anti-corruption in public procurements arises not just from its technical novelty. Rather, its relevance rests upon its unique architectural principles of decentralization, transparency, and auditability, each of which addresses particular structural deficiencies in procurement governance. Each of these features targets a distinct corruption vector: a centralization of control, an opacity of information, and an absence of trustworthy accountability. Individually and collectively applied through its integration to create an ecosystem of procurement workflows that help maintain integrity at the system level, reduce administrative discretion, and leverage real-time accountability. This section will unpack the conceptual basis and applied meaning of each, and show how the simultaneous application of these principles can engineer procurement systems that are procedurally resilient and institutionally trustworthy.

I. Decentralization: Erasing Discretion and Fragmenting Authority

In traditional procurement frameworks, almost all forms of authority are thrust into a limited hierarchy of ministries, agencies, or contracting authorities that dictate bidding, award determination, and payment distribution. This clearly consolidates discretion, creating opportunities for similar opportunities to exhibit bias, gatekeeping, and to solicit bribes (Rose-Ackerman & Palifka, 2016). Blockchain decentralized networks disrupt this governance structure through independent third parties since transactions are validated through not a managing authority, but a consensus or group of independent nodes—these nodes can be inter-agency, government, or independent monitors who share a common purpose that are disassociating power, negating control, and/or limiting unchecked or unilateral conduct.

In a public procurement framework, and in permissioned blockchain, decentralization is not solely an open-ended process: nodes are established and vetted actor (such as procurement regulators, ministries of finance, or anti-corruption agencies) that can validate transactions. These participating nodes reflect institutional accountability through independent vetting while promoting an accountable and robust resilient network. Another service provided by decentralization is the ability to create interoperability across competing procurement jurisdictions, or when countries have a federal system like Canada or the United States. Decentralization techniques will allow for synchronized blocks of procurement-related events to occur through many levels of government.

That being said, decentralization is not a cure all. It creates the institutional structures of governance to limit elite capture of nodes and must have structures for defining consensus, conflicts, and institutional authority. Absent these structures, decentralized architecture is in danger of becoming distributed bureaucracies, marginally spread out and uncoordinated.

The concepts behind blockchain decentralization, transparency, and auditability, are not just theoretical concepts and examples of how those constructs have been put into action in real procurements systems are evolving daily. In Europe, the National Anti-Corruption Authority (ANAC) has conducted pilot tests of blockchain technologies within a public procurement context to increase transparency and accountability. The National Public Procurement Database (BDNCP) is using blockchain technology on an applicant's proposal and the awarding of contracts and payment disbursements to create tamper-proof digital records, a move which will curb manipulation (Galli et al., 2023). In Canada, Public Services and Procurement Canada (PSPC) has also begun to used blockchain on projects to increase contract management efficiencies based on real-time accountability and automate compliance (Government of Canada, 2023). In the USA, the General Services Administration (GSA) and the Department of Defense are researching smart contracts, which will automate compliance processes by ensuring that that payments will only be authorized based on completing contractually defined milestones to minimize both fraud and delays (GAO, 2023). In total, all of these developments, suggest that the features of blockchain – decentralization, transparency, and auditability – will be incorporated into procurement practices remove corruption risk while increasing efficiency.

Nevertheless, although there is a will and professionalism to change, there are significant legal barriers to overcome. In particular, the EU General Data Protection Regulation (GDPR) has a serious problem with the right to be forgotten, which hinders blockchain's immutability features. As is the case with many variations of the European Blockchain Services Infrastructure (EBSI) - while there are some privacy elements insofar as zero-knowledge proofs, there are still outstanding issues around whether to keep some data and whether users have a right to have data not retained or deleted (Zetzsche et al., 2017). The USA and Canada present similar issues. In Canada, for example, legislation such as the California Consumer Privacy Act (CCPA) identifies "personal data," while the transparency of blockchain's officiating commands will need to be re-evaluated, as well as off-chain data maybe a way forward for being able to observe privacy laws while providing users the benefits of blockchain (Bradshaw et al., 2019).

These legal barriers will prove difficult to overcome but the more pressing challenge now is to overcome 'buy-in' issues for the adoption of blockchain for public procurement. The interests of procurement officers, politicians and vendors all meaningfully attach the legitimacy of the existing public procurement system to the continued retention of transparency and compliance information available when that power of ease is removed/mitigated from these stakeholders entire - creating an entirely automated process (Bovaird & Löffler, 2016). In Italy, the interests of the vendors are entrenched within the opaque nature of the public procurement system and may create a rational dread of 'losing their monopoly' while blockchain is used, from the angled perspective of their competitors the potential fallout include competition using the same procurement approval algorithms. Additionally, in geographically democratic federal jurisdictions of the USA and Canada, due to size, it creates another layer of complexity in creating blockchain interoperability between levels of government. There will be significant barriers to an aligned use of blockchain due to the number of regulatory levels at: federal-side (federal, state, provincial) and in both Canada and the USA in, necessitating cross-jurisdictional cooperation to create interoperable solutions (GAO, 2023).

It must be noted that there is a detailed plan to overcome all of these barriers, which must include stakeholder engagement, capacity building and aligned polity. Ideally, if those who wish to advance the blockchain implementation agenda wanted to win they should enter into the new debate context leveraging the existing legal institutional context, as well as being open to thinking with both technological and institutional constraints (Bovaird & Löffler, 2016). It is advisable to take small steps slowly, with pilot programs and regulatory sandboxes so that damage to all stakeholders can be diminished as it goes through the testing of the blockchain solution to navigate the associated legal and institutional barriers.

II. Transparency: Disrupting Opacity via Verifiable Disclosure

Transparency has always been a core principle of public procurement reform. However, operationalizing transparency so that it provides genuine benefits continues to be inconsistent. The information regarding tender opportunities, evaluating criteria, contract terms, and agreement

outcomes is often received late or poorly or not available at all, allowing for actors to change their documents, hide noncompliance or bury red flags. Blockchain is offering a new method of programmable transparency: every movement in the procurement process (for example, tender publication, bid receipt, notice of awarded or milestone delivery) will be logged as a time-stamped, immutable record on a shared ledger that can be reviewed by all legitimate participants and the public in appropriate cases.

This kind of system-level transparency lessens information asymmetries amongst government, suppliers, auditors, and civil society. It also allows for supervision or oversight to be at level of near real-time, because it does not require any reliance on ex-post or relying on post-disclosure audit events. As an example, bids submitted via a blockchain-based bidding system would have all bids available for automated disclosure once the submission deadlines are completed; going back and making entries or faking quote wouldn't be impossible. This is an extremely important capacity in environments where the procurement has always been the vehicle for political patronage or clientelism (OECD, 2016).

The need for transparency, however, needs to be balanced against legal and ethical considerations, such as data protection, commercial confidentiality, and procedural fairness. Together, all procurement data should not always be publicly available in the entirety. Therefore, blockchain-enabled public procurement and contracting systems will have to incorporate selective disclosure protocols from the start and more private cryptographic tools — zeros-knowledge proofs and hashed references — to ensure compliance and privacy within legal frameworks (GDPR) and protect bidders' rights.

III. Auditability: Preserving Institutional Memory and Preventing Manipulation

Procurement systems operate only to the extent that they capture, recall, and validate transaction life cycles. In many jurisdictions, inadequate record-keeping and tampering of records eliminate audit effectiveness, enable unsavory actors to erase the disposition of corrupt activity, and undermine court enforcement. Blockchain's immutability directly confronts this problem. Once validated, entries on the ledger are tamper-evident, and all entries are permanently linked through hashed cryptographic hashes, hence the procurement actions are recorded clearly and cannot be changed without transparency (Zyskind et al. 2015).

This pernicious documentation refers back to ex ante compliance monitoring - from the perspective of staff supervisory personnel to find out about procedural irregularities as deviances occur, and ex post forensic auditing that requires high-quality, sequential evidence (potentially for litigation investigation). For example, consider an instance, of a payment released without a corresponding verified milestone - auditors will see the irregularity immediately. They will then have to follow the chain of entries to determine the origin of the mistake. Logically, the audit chain forces a liability on all players at every level of procurement chain, from budget allocation to final payment.

As previously mentioned in this discussion, necessary correlations between blockchain entries and legal creditableness remain a challenging issue for all legal systems. In the case of Italy, where civil law is the legal dominant and where the encumbered age amalgamations of statutes may require active reference to clear any necessary standards governing usage of blockchain records, establishing admissibility of entries as probative legal evidence and clear purposes will be vital. In addition, procurement systems must incorporate processes which annotate or contexture ledger entries, particularly in relation to verifiability issues delegitimizing impact on contract variations, force majeure and administrative error.

IV. Anti-Corruption Synergy: From Principles to Systems

From a summative perspective, decentralization, transparency, and auditability are discrete object integrity enhancing disciplines; when they couple together, they represent a systems redesign reformulation of trust and accountability in procurement governance. Decentralization obfuscates capture and gatekeeping; transparency reduces discretionary concealment; and lastly auditability contributes to procedural fidelity and forensic enforceability. When built into the digital architecture of procurement or integrated in customizable procurement platforms, reformulation has the potential to reshape corruption control from a reactive enforcement dilemma to proactive systems design intent.

For countries like Italy, Canada, and the United States, embedding of these principles must occur within the legal forces, political culture, and capacities of public institutions. Italy, as previously mentioned, will need to address the means of legal encoding of blockchain records within their statutory framework, as a civil law practitioner I can imagine a statutory process operating through a standardized notion used to ensure that blockchain records use the same principles of notarized documents or stamped certificates. Canada’s multi-guerre intergovernmental procurement, through multiple jurisdictions will need operating transparency, similar protocols must be established and accessed through interoperability across platforms at both provincial and federal platforms. Alternatively in the United States - with diverse yet bureaucratic agencies - strategic use pilot programs that take in auditability and decentralization in a staggered or incremental systematic approach to projects within federal acquisition can maximize their potential.

Ultimately, as consistently stated earlier, blockchain’s promise of anti-corruption lies not only in the technology of its indiscriminate uniqueness, but primarily in its operationalization of the constitutional principles underpinning procurement, principles of fairness, openness, and accountability can be written as features of a formally coded system; rather described as principles and anticipated as theories. In a blockchain environment these will be enforceable through cryptographic certainty, automated consensus implementation, and because transparency is immutably linked to the procurement functions of the system, traceability is assured.

3.2.2. Smart Contracts, Automation, and Legal Enforceability

In the context of reforming public procurement systems, probably the most exhilarating yet controversial blockchain characteristic is the smart contract - a computer code that acts as a protocol that self-executes according to specified conditions and enforces an agreement. As an operational innovation, a smart contract displaces the enforcement of a contract from ex post enforcement through legal institutions for ex ante enforcement via technology. Smart contracts seek to eliminate bureaucratic discretion, eliminate waiting times and eliminate loopholes that are typically exploited by corrupt actors and inefficiency. In public procurement systems, where there is typically an array of non-compliance with contract conditions, post-award renegotiations, or altercations whether payment is earned - the automation resulting from smart contracts can deliver a structural solution of conditionality through tamper-proof execution. Implementation risks anticipated risks of compliance with the contract and at the same time introduce the principal characteristics of an "automated" technology-enabled solution. Smart contracts must be evaluated against legal, administrative and organizational dimensions, even for those traditions of civil and common law. The schema of a smart contract is not its automation as a potential innovation, nor to be useful, is dependent on its availability for the normative consideration of public procurement regulations in states where legality, fairness and due process must coincide with technical efficiency in a legal distribution of public finances.

The traditional arrangement known as the public procurement contract is a binding agreement (known as a contract) made between a supplier and a public entity under administrative law, and broader regulation (e.g., rules of public finance and national procurement codes). Public contracts can be subject to scrutiny by contract controls including parliamentary appropriations, rules and regulations on procedures, oversight exercised by auditing penalties and context for recourse against a public investor through legal adjudication. In Italy, for most jurisdictions of public law, including commonly civil law system, public contracts are also reconciled with a law metric of procedure, especially the law of process - over and above hierarchical measures of legality (Gabor & Casalini, 2021).Within this context, the adoption of smart contracts presents a fundamental question: can legal obligations be validly and adequately represented in machine-executable code, in a way that does not compromise the foundational legal concepts? Smart contracts may improve enforcement timeframes or create sensitivities to discretion, but their utility in the public sector will be determined by whether the automated logic embedded in a smart contract is legally enforceable, procedurally accountable, and institutionally trusted.

In principle, smart contracts are compelling anti-corruption devices. Their automation aims to be able to avoid unauthorized contract modifications, deliverable milestone-based obligations, and only disburse funds when outcomes are pre-determined and verifiable. If successful, these smart contracts will reduce the ability of procurement officials to vary payment times, include inflated invoices, or offset the requirement of delivery – behaviors commonly seen in corruption cases involving inflated payments, non-deliveries, or false invoices (Rose-Ackerman & Palifka, 2016). For example, a smart contract for delivering infrastructure may automatically release progress

payments based on a verification of completion at various stages in the project process, by an independent engineer, where the verification and independent engineer's digital signature, which is recorded on a blockchain, fulfills these obligations. Thus, a smart contract reducing opportunities for corruption is provide by removing manual touchpoints, which are more easily manipulated for compliance verification, as well as automating reliance to contractually encoded compliance mechanisms.

Nevertheless, the legal enforceability of smart contracts in public procurement is still an open question in many jurisdictions. Under common law, as in Canada and the United States, contracts can typically be legally enforced if they can demonstrate the elements of offer, acceptance, consideration, and intention to create legal relations. Courts have begun to recognize electronically formed agreements and smart contracts as enforceable according to contract principles, once the terms are clear and parties are willing to assent (Werbach & Cornell, 2017). Some states in the U.S., such as Arizona and Tennessee, have passed laws regarding the legal validity of blockchain-based records and smart contracts, but these laws are generally limited and do not address public procurement specifically. In civil law jurisdictions (such as Italy), legal compliance may be more difficult to demonstrate. The Italian procurement code, as an extension of the administrative law tradition, imposes centralization, ex ante legal authority, and judicial authority over any variance from the statutory sequencing. Prescribed procurement processes that follow the code generally involve human input at all steps. The execution of obligations under the contract is attached to the status of hierarchy matched with legal rules, not coded instructions. Also, as discussed earlier, public procurement is not solely transactional; it is also a sphere of public governance where accountability, equality, and proportionality are conspicuous factors that require implementation. Any automatic smart contract to facilitate payments complicates the supplier's right to be heard regarding a performance evaluation or challenge the legality of the termination clause. Public procurement contracts, as we noted, are not based on a free market but rather on prescriptive legislation, competitive procurement procedures, and legislative standards which may invoke the constitution. In other words, automation, even when removing discretion, can also jeopardize legal structures, if the individual pacing is not considered. An unyielding contract without contingency clauses and room for interpretation has the potential to result in an inequitable outcome or purchase failures, such as price fluctuations, supply chain disruptions and natural disasters (Corrales et al., 2019).

One potential response to these issues might be hybrid contracts that integrate machine-readable logic with legally binding, human-readable terms. The "dual-layer" contracts retain the automation advantages of smart contracts, while still retaining the legal protections and interpretive flexibility of existing traditional public law tools. In this contract model, the smart contract will perform the standard verifications, such as bid submission deadlines, milestone payments, and delivery verification, while the underlying legal contract will govern the substantive terms, exceptions, and dispute resolution. This compromise has been proffered where regulation dictates an operational balance between legal protection and operational efficacy (Finck, 2019). Public agencies wanting

to use smart contracts need to be incentivized to prototype modular, auditable systems in experimental environments like digital innovation labs or regulatory sandboxes.

Operationalizing smart contracts in public procurement entails establishing a fundamental shift in institutional capacity. Agencies will need to develop skills in modeling contracts, algorithmic design and auditing systems. In addition to legal compliance training, procurement officers require capacity training in how that employs smart contract structure, for example, the conversion of legal clauses into programmable rules through the code. Oversight institutions will need to have the ability to assess and audit contract logic and vulnerabilities and to evaluate the legality of digital contracts with procurement legislation. The situation is pressing particularly in countries where the digital infrastructure and human capital technology are still developing. Italy made advancements in e-procurement and digital identity infrastructure; however, it still lacks an adequate legal framework for blockchain in public administration. Public Services and Procurement Canada (PSPC) has begun to investigate digital procurement reform in Canada, although they are not yet willing to fully automate procurement due to concerns regarding transparency and accountability. In the USA pilot projects by agencies including the General Services Administration (GSA) and Department of Defense have sketched out the potential for integration of a smart contracting model, but implementation is experimental and fragmented.

To summarize, and with regard to the social and political elements of automation in public procurement, it is widely recognized that automation introduces a different type of opacity—that of algorithmic opacity-- wherein the decisions might become irreconcilable or impervious to contest, especially when the coded logic is unavailable for review to non-technical stakeholders. The public's trust in procurement processes relies on a variety of things, including the absence of corrupt practices and the ability to comprehend and contest decisions viewed as unfair. If smart contracts are developed without regard to feedback mechanisms, error correction processes, or overrides, the unwillingness to engage and alienation of external third parties could cause stakeholder alienation and lessen perceived institutional legitimacy. As a result, successful implementation would be predicated on (a) legal harmonization, (b) accurate logic, and (c) the application of participatory design principles and accountability mechanisms that maintain the democratic principles of public expending.

In conclusion, whilst smart contracts offer a compelling but highly contingent solution to procurement corruption, their ability to automate compliance, performance conditions and hold accountable non-discretionary manipulation are a perfect fit to long-standing failures in procurement oversight. But such success relies on more than logic. They need to be interpreted, validated and legitimized within established legal frameworks, administrative practices and governance cultures. For this reason, the adoption of smart contracts in Italy, Canada and the USA will need to be approached as legal-institutional change, rather than a technical implementation. The comparative approach offered in this dissertation offer insights into how smart contracts can be deployed not just efficiently but also legitimately and accountably across disparate procurement systems.

3.2.3 Data Integrity, Immutability, and Trust in Procurement Processes

In public procurement systems, data integrity is a key element of procedural legitimacy, financial accountability, and administrative sustainability. There are a number of stages in the procurement process generating a system's data, from announcements of tenders to final payments of bills and all steps in between, and this data must be accurate, verified, and available to the public and/or auditors to ensure legal compliance and institutional accountability. However, unless these systems are particularly strong - which is rare - many procurement regimes, especially those operating in fragmented bureaucratic environments with limited capacity, struggle to maintain complete and unalterable records. The absence of correct document management, information asymmetries, or a lack of oversight can create the opportunity for corruption (through distortion of records, loss of the audit trail, and deletion of 'compromising' documents). Blockchain is a form of technology that may offer potential remediation for these persistent shortcomings in existing procurement regimes as it includes the concept of immutability. The immutability of blockchain provides a way of protecting procurement data in a form that cannot be erased, which promotes improved internal accountability as well as external transparency.

Immutability in the context of blockchain is generally understood as the structural and cryptographic safeguards which indicate that recorded data can be neither retroactively changed or erased. Every block of information in the blockchain has a link to the previous block in the form of a hash function, which means that if a block (record) is changed, the hash would also change. The chain can only be trustworthy if a change to the records is authorized across the entire network planted, or distributed then propagated as an accepted record. This characteristic of blockchain is especially useful in public procurement. In using the blockchain, once a procurement action is recorded (issuing the tender, submittal for purchase, and approval to pay), that record cannot be unverifiable altered. The permanent sequence of events can prevent practices such as backdating contracts, biased deletion of documents, or tampering with evaluations. As a result, the issue of corruption around data manipulation is alleviated, including falsified documents, lack of a paper trail, and "paperless" payments that go unchecked (World Bank, 2020; Mathews et al., 2022).

The need to preserve data integrity in procurement is not solely for the prevention of corruption. Reliability is also fundamentally important to evidence, dispute resolution, and institutional evaluations for long term policy. Issues with document retention, available records, and standards can plague traditional procurement structures, preventing not only future monitoring, but also retrospective examination, and organizational learning. Blockchain's structural rigidity responds to the document retention and access challenge, and can consistently present one immutably recorded act, linked in chronological order, available for authorized users in real time. These processes can strengthen the assurance and completeness of procurement records, allowing different departments to coordinate actions better, and the ability to reactively administer governance in multi-level environments. It can also continuity against intervening organizational change and retention ability in contexts with significant employee churn and new elected officials (Finck, 2019; Janssen et al., 2020).

Data immutability performs a similar, although not identical purpose, for legal and evidentiary purposes. In many jurisdictions, but especially those with weak institutional checks or oversight, having to mount a case on procurement corruption is predicated on the quality and integrity of documented evidence reflecting decision-making. Blockchain's immutable records provide a real evidence trail in ways available to agency officers with mathematical proof of how and where a fraud did or did not connect. For legal professionals, this means that verifying facts can happen freely of institutional control and political influence. For auditors and investigators, blockchain data systems provide a method of reconstructing elaborate chains of transactions and can trace any anomalies of procedure precisely in both time and forensic context (Zyskind et al., 2015). In this way immutability enables both ex-ante accountability and ex-post enforcement.

Importantly, while immutability provides strong assurance against unauthorized adulteration, comes normative and legal tension. Absolute immutability may breach widely accepted public law principles, in particular the principles of administrative discretion, corrective measures, and the forgetfulness principle. the proscribed-forgetting principles codified in the European General Data Protection Regulation (GDPR) states that individuals must have the capacity to request the termination of personal data in certain situations contrary to immutability forever present on blockchains. Likewise, in administrative processes, they may confer the right of appeal or exceptions based on new evidence or legal reinterpretation. Procurement decisions, when already hard-coded and willfully stored immutably, creates a blockage to the ability for public authorities to comply with political expectations, court orders and mandates (Finck, 2019). These tensions indicate the important need for governance mechanisms changing to support flexibility necessary to meet prevue duties; doing so however without undermining the essential principles for which records are contemporaneously maintained.

A number of architectural solutions have been advanced to allow lawful flexibility without detracting from immutability. One solution may be where sensitive or particularly amendable data is stored off-chain, and only a hash of relevant on-chain data is stored to satisfy the corresponding on-chain verification. This allows for data to be modified or deleted in compliance with legal obligations while ensuring that any modification can be identified and justified. Another approach is to employ permissioned (or "private") blockchains where only vetted institutions write to the ledger and changes are ratified through a defined set of consensus rules. More elaborate governance mechanisms can involve layering override protocols - such as digital signatures from oversight institutions or timestamped annotations indicating the legal justification for a change made retroactively. These methods allow for auditability while ensuring that blockchain-based procurement systems can clearly function amid broader constitutional and administrative rules of democratic governance (Zetzsche et al., 2017; Corrales et al., 2019). The advantages of data immutability also pertain to the value for public trust. In many nations, trust in procurement systems has been undermined by perceptions of opacity, manipulation or impunity. Citizens, suppliers, and civil society actors assume that procurement documents can simply be deleted or altered to protect favored bidders or to obscure unlawful behaviors. By providing a verifiable and

transparent system where users can appreciate procedural data that is immutable and publicly available, blockchain systems can serve as infrastructure to help to restore public trust. This is not simply a technological benefit, but a democratic benefit. A citizen's confidence in public institutions will be contingent on ethical leadership and success navigating their obligations, but also on the integrity and permanence of information (Atzori, 2015). When citizens take comfort in knowing that procurement data is incapable of being clandestinely manipulated or erased, they will believe there are legitimate reasons and less likely to assume political favoritism is at the root of outcomes delivered.

From a cross-national perspective, the institutional implications of blockchain-enabled data assurance vary considerably depending on legal traditions, administrative architecture and technological capacities. In Italy, for example, procurement mischief has historically existed by way of being able to falsify or eliminate significant records, often at the sub-national domain. By adopting immutable ledgers, it is conceivable that audit reliability could be considerably enhanced and the presence of evidence in a court would be that much richer. Again, this would be subject to the notion of being consistent with GDPR, principles of administrative law and EU procurement behavior. Canada, as an example of a federation with multiple levels of procurement authority, similarly would benefit from immutable records to facilitate coordination and traceability between jurisdictions. The challenge of agency here would not only be technical but as articulated, regulatory providing blockchain systems meet interoperability with existing data standards and compliance with legal obligations. In the USA, in circumstances where contracts require high-volume activity, blockchain could offer a proof-based defense against being manipulated for fraud by vendors at the state or municipal level. Yet interoperability, admissibility and scalability remain significant issues.

To sum up, data integrity and immutability offered by blockchain reinforces a significant and persistent weakness experienced in public procurement systems was vulnerability of records to corruption, loss, and manipulation. By embedding procurement data in an immutable, verifiable, and distributed ledger, blockchain promotes both internal accountability and public trust. Technical immutability will not ensure there are legitimacy, however. That being said, blockchain systems will only function effectively if the processes are configured into existing legal structures, norms of privacy, and levels of institutional flexibility needed by democratic norms of procurement. When configured and governed at the appropriate level, immutability becomes a characteristic of the digital infrastructure as well as a fundamental principle of procedural justice and institutional legitimacy in the public procurement process.

3.3.1 Legal Traditions and Contractual Enforceability (Civil vs. Common Law)

The inclusion of blockchain technologies in public procurement is heavily influenced by the legal frameworks and traditions in which public procurement operates. Legal traditions condition the form and interpretation of contracts; and the legal traditions influence the administrative process

of expenditures, how the procurement is overseen and assessed and, dispute resolution. Therefore, legal traditions are key to understanding the efficacy of blockchain-based solutions (e.g., smart contracts or immutable blocks) so they may be legally recognized, enforced, and practically executed in different jurisdictions. The study of public procurement and blockchain technologies will focus on two primary legal families, the civil law tradition, with emphasis on an example country Italy, and the legal common law family with notable examples including Canada and the United States. Legal families have distinct interpretations of contract law, administrative processes of governance, and how judicial review is applied; and these differences mediate blockchain feasibility within public procurement context.

Civil law traditions base in written laws, comprehensive legal codes, and an emphasis on the formalism of the law and hierarchical legal authoritativeness, for instance, in Italy, public procurement is governed by the Codice nuovi contratti pubblici (Legislative decree 50/2016) that proceeded outcomes of European Union (EU) procurement, particularly Directive 2014/24/EU and the legal ramifications of the principal law of the EU. The codified rules and regulations under the Codice for public procurement delineate significant precision in the procedures for public procurement including; the publication of tenders, evaluation and award of contract, administration process of review if tendered for, and the scope for consideration of the procedural legality, transparency and fairness of the procurement process (Monteduro, Hinna & Moi, 2016).Under civil law, written contracts, formal approvals, and documents signed or stamped are traditionally relied on as evidence of validity and binding nature. Contracts, when reduced to a contract governed by smart contracts, and documents stored in a distributed ledger with immutability, raise the question of interpretive legal validity, especially in statutes or regulations related to public contracts given civil law's prescriptive administrative controls and limited judicial discretion. This leads to the question of whether smart contracts and blockchain records meet minimum legal requirements for public contracts in civil law systems (Savelyev, 2017).

In comparison, common law in Canada and the United States is less prescriptive with varying degrees of interpretative flexibility given case law reliance. Contractual obligations are governed by case law interpretations and precedent, with focus on intent of parties; mutual assent; and performance obligations. Such interpretative flexibility may favor the ability to legislate and judicially recognize smart contracts and blockchain records as long as essential contract components are satisfactory under jurisdictional definitions for: offer; acceptance; and consideration (Werbach and Cornell, 2017). Some U.S. states have introduced legislation recognizing blockchain and smart contracts, providing public agencies freedoms to test out digital options for contracting (Marinos, 2020). Canada generally follows common law however federally legal pluralism exists in personal property by Quebec's Civil Law. Meaning any blockchain uses must comply with both systems when jurisdictional shipping occurs, making developing interoperable and legally compliant e-procurement systems difficult (Gow and Paré, 2021).

Common law jurisdictions can allow flexibility; unique legal issues exist. The questions about liability attribution in automated transactions, whether code is adequate as evidence in a dispute,

and what procedural safeguards are required to fulfill legitimate public interest remain largely unanswered. While smart contracts are automated and self-executing, issues surrounding discretion and human judgment that are common to public law remain critical to specific administrative procedures to assure accountability. The different levels of technological readiness and standards further add to the complexity (Clack, Bakshi & Braine, 2016). So, even where more liberal and innovative approaches thrive, legal instruments, frameworks, and administrative procedures must adapt to define the relevant responsibilities and protections against fraud and abuse in blockchain-enabled procurement.

The legal culture, comprised of social perspectives regarding law, the behavior of legal actors, and the procedural norms that guide legal action, is another salient factor applicable to blockchain. Legal culture in Italy - as in most civil law systems - is complex and often characterized by a strong emphasis on formal procedure and centralized control or authority, as such enhances expectations over the speed of new technology in initiating the points of change in public administration. Legal conservatism and bureaucratic inertia (Nelken, 2004) contribute to rigidity in the adoption of the blockchain, especially in contexts involving significant or high-value public expenditure. In this sense, a legal culture in Canada that embraces pragmatism and a tendency to allow for market-based innovation in public procurement (Pistor, 2019) also pragmatically invites new forms of governance tools - including blockchain. Accordingly, a comparison of the values inherent in the legal culture helps anticipate the taxonomy of institutional receptiveness or resistance that blockchain - at least beyond the mere statutory layout.

Overall, the context around legal traditions from civil and common law systems provide comparative regulatory environments around blockchain-enabled public procurement. Civil law systems emphasize formality through codification processes which may require legislative changes or interpretative directives to facilitate blockchain's typical forms of novel contracts. On the other hand, common law may not engage the same level of formality; however, it is stymied by automation against legal principles rooted in state accountability, and human discretion. The comparison of Italy, Canada, and the United States shows that the legal compatibility of new technologies is a product of both jurisprudential culture and institutional capabilities as much as its statutory design and expression. Thus, the implementation of blockchain for anti-corruption in public procurement cannot merely be driven by technological innovation, but with concurrent legal and institutional alignment adapted to the context of governance.

3.3.2 Adaptive Policy Transfer and Institutional Readiness

The acceptance and use of Blockchain technology in public procurement is best thought of as being part of adaptive policy transfer and institutional readiness. Policy transfer is defined as the process, where policy, administrative, or institutional knowledge are drawn upon in one setting based on experience in another setting, where adaptation is required, taking into account the local legal, political and administrative context (Dolowitz & Marsh, 2000; Bache & Flinders, 2021). This is of particular relevance in terms of emergent technologies such as blockchain, which require

challenging tensions of legal norms, technical standards, and governance cultures. Successful policy transfer is uniquely contingent upon the readiness of the institution, which include legal capacity, administrative practices, digital maturity, cultural artefacts and willingness of stakeholders to support and champion innovation (Rogers, 2003; Zhang et al., 2022).

Institutional readiness can be viewed broadly, referring to global capabilities which exist at both the concrete level (e.g., technology infrastructure and processes) and an abstract level (e.g., organizational adaptability and adoption of a culture of innovation). Jurisdictions with high e-government maturity, future strategic directions for digital transformation, and existing units specifically for innovation are the best candidates to run pilots and scale Blockchain applications for public procurement (Canada Digital Service, 2023; OECD, 2022). For example, Canada is a country that has invested heavily in public sector digital modernization, including the institutionalization of innovation across central agencies, that increasingly include new technologies, including blockchain (Government of Canada, 2023). This tendency to be proactive is important for iterative experimentation, which includes feedback loops and adjusting blockchain actions to meet the needs of local governments. Effectively this gives rise to more effective transfer on both contextual fit and absorption capacity.

In contrast, institutional complexity and legacy administrative practices constrain blockchain adoption where stakeholders may not have a strong institutional readiness orientation, as can be seen in Italy's public sector. Italy has made important strides in the use of digital technologies to scale, optimize and formalize procurement practices. Examples include moving quickly to fulfil the requirement of the European Union directives like 2014/24/EU directives to digitize procurement as much as possible. However, Italy's environment of bureaucracy is filled with sometimes ambiguous bureaucratic domains of competence that overlap at national, regional and municipal contexts tied to a traditional formalistic culture (Rinaldi & Bertuzzi, 2022). This environment generates inertia in procedures, fragmentation of policies and comprehensible procedural weakness that could streamline public procurement yet hinder its successful implementation on a cohesive level. However, various supranational entities, like the European Blockchain Partnership, and other digital governance mandates for the EU, have significant pull to incentivize their Member States to seek solutions along the path of blockchain potential features. Italy's manifestations illustrate an adaptive transfer process combining domestic institutional constraints and supranational pressures for modernization new technological directions (European Commission, 2022).

The United States provides a different model for exploration. The U.S. offers a decentralized governance model that excites innovation within the nature of its governance structure. In the U.S., designated procurement activities are distributed throughout federal agency responsibilities and similar designations at the state and local levels, where institutional readiness mapping is varied (GAO, 2023). Yes, innovation hubs like the General Services Administration led pilots of Blockchain, supporting experimentation and pursuit of innovation, however, other agencies and states still experience a variety of capacity gaps, and strategic ambiguity that inhibit a process that

would optimize technology adoption as an efficient and effective tool (U.S. Office of Management and Budget, 2021). Every nascent ecosystem is capable of encouraging public–private partnerships and innovation ecosystems that support knowledge diffusion and policy learning, both important aspects of adaptive policy transfer necessary when you combine innovation, technology, and social context (Mason & Webb, 2024). However, this decentralization allows for localized experimentation, while also necessitating those in jurisdictions share strategies that support the scaling of innovative practices as a consistent model of implementation across jurisdictions though carefully shared coordination processes. Institutional readiness is greatly influenced by socio-political issues such as hierarchical inertia and bureaucratic norms (Bovaird & Löffler, 2016) that create resistance to change, labor union concerns, and skepticism from suppliers that an existing procurement problem will be solved. Effective transfer and adoption of blockchains in public procurement, therefore, require the development of legitimacy under transparency and governance that are legitimate to multiple actors. Participatory models involving users, civil society organizations, private sector interests, and oversight actors build trust and create collaborative ownership of blockchain proposals (OECD, 2022). Belonging internationally, for instance to Trans-Jurisdictional Knowledge Exchanges, that bolster institutional capacity are critical to enhance the potential for transfer and share experiences of best practices, lessen risk, and hasten learning cycles (Zhang et al., 2022).

The emergence of regulatory innovation supports institutional readiness in ways that create space for experimentation. Regulatory sandboxes—experimental spaces to try out new technologies in relaxed parameters of legality—are an emerging method for navigating uncertainty and developing responsible innovation practices with technology (Zetzsche et al., 2023). Canada's development of regulatory sandboxes for fintech is a particular use of a sandbox and exemplifies how a sandbox might likewise enable blockchain applications in public procurement by establishing an equilibrium between innovation and risk (Canada Digital Service, 2023). The European Union is developing conditions for experientialist governance which facilitate even greater iterations of policies in participants sharing similar legal and administrative frameworks. In the case of Italy, iterative public blockchain implementations could co-existing focus on achieving a significant in-place understanding of blockchains new legal and administration framework (Sabel & Zeitlin, 2019). The US has engaged decentralized use of consensus in labs and pilot programs to idea test blockchain technology—each use case has built a fantastically layered experiment of introducing blockchain ingenuity within the fragmented governmental narrative (GAO, 2023).

In conclusion, institutional readiness and adaptive policy transfer are consequential areas for understanding blockchain technology as part of the implementation of public procurement reform in varying contexts. We have discussed Italy, Canada, and the United States—and provided examples of their institutional configurations and capacities that might influence their technological adoption trajectories. Recognition of, and understanding these differences is a core consideration of how we can develop blockchain technology that both satisfies technology

adoption but is also sustainable as an institutional innovation. Once the technology satisfies user experience in adoption, this enables richer conversations about the functionality of blockchain in achieving meaningful change towards the ending the establishment of corrupt practices, or public sector modernization reforms.

3.3.3 Multi-Level Governance and Cross-Border Implementation Barriers

Public procurement systems exist within complex governance architectures that extend beyond the capacity of a single government, and the term multi-level governance expresses this complexity by combining supranational, national, subnational, and non-state organizations as actors in the delivery of policy and implementation of regulation (Hooghe & Marks, 2001). To make sense of the multi-level governance dynamics is significant in order to assess what challenges and opportunities the use of blockchain technology encounters when used to combat corruption in public procurement across different jurisdictions. The interdependencies of governance levels affect, therefore not only the technical operational capability of blockchain systems, but also the legal, administrative, and political legitimacy of such systems.

At the supranational level, the European Union represents a governance architecture in which the EU has an enormous impact on the procurement of its member states. For example, the EU has developed procurement directives, with the most well-known being Directive 2014/24/EU which sets out harmonized rules on transparency, non-discrimination, and competition in the internal market (Trybus, 2014). EU directives require member states to develop a procurement system where rules mandating a formalized process are defined – e.g., publication of tenders, assessable criteria for evaluating tenders, the route to remedies, etc. Any blockchain-based procurement platform will need to develop regulations to comply with this EU regulatory architecture while complying with domestic regulations taken from the EU rules. Although the EU is promoting interoperability and digitalization across public procurement practice for its members to use blockchain solutions, the advancement of different levels of legal standards and administrative maturity will limit its implementation potential (Finck, 2019). Furthermore, the data protection provisions of the General Data Protection Regulation (GDPR) impose limitations on handling of data within blockchain systems which necessitate administrative solutions to develop technical measures capable of linking immutability and privacy rights (Kuner et al., 2019).

The matter is complicated at the national and subnational levels. For example, in federal systems such as Canada or the United States, the procurement authority is spread over federal, provincial/state and local agencies and an agent has its own rules and procedures which vary throughout the three jurisdictions. This creates challenges adopting a uniform blockchain system across many organizations while the likelihood of cross-jurisdictional procurement requiring coordination of processes, information and legal considerations appears to be high (OECD, 2017). In Canada, one cannot impose procurement policies over their provincial counterparts if the two jurisdictions have different legal foundations, capabilities or agendas. The incentive to resolve this heterogeneity through solutions is often in the form of interoperable platforms and standardized

protocols (Government of Canada, 2020). In the case of the United States which has intricate federal-state relations, it is bound by agency-specific Federal Acquisition Regulation (FAR) obtaining competing agencies rules across the various tiers of government. The United States has seen pilot programs in blockchain but patterned-wide adoption of blockchain procurement systems is complicated creating a unified national entity (GAO, 2020).

Cross-border procurement exacerbates the complexities of governance systems. International tenders, bilateral trade, and multinational public–private partnerships all require procurement systems that can maneuver different legal systems, regulatory frameworks, and data governance regimes. While the potential of blockchain is a unified, tamper-proof ledger, it is often hindered by national limitations dealing with the enforceability of contracts, electronic signatures, data sovereignty, and privacy legislation (De Filippi & Wright, 2018). For example, if jurisdictions recognize a smart contract's validity differently, such as whether it's the same as a traditional contract, then the legal certainty in the cross-national procurement contract is reduced. Similarly, while data sovereignty laws may instruct data localization requirements at the national level, additional laws implemented to maximize cybersecurity may restrict the transmission of procurement data located on a distributed ledger (Bradshaw et al., 2019). Conclusively, these regulatory hurdles indicate a need to create governance structures that create coordination, standardization, and mutual recognition among states and their agencies.

Nevertheless, multi-level governance frameworks can facilitate favorable conditions for the deployment of blockchain technology. Supranational institutions and international organizations generally adopt a more expansive facilitative role in enacting changes, rather than executing regulatory systems at the national level. For example, supranational institutions look to fund pilot programs to act as proofs of concept, set standards, and encourage interoperability through experimentation (European Commission, 2021). The European Blockchain Partnership, for example, aims "to create common infrastructure (including layers of interoperability) and develop common regulatory guidance that will support interoperable blockchain systems across the EU" (European Commission, 2021). Similarly, while the OECD and World Bank are working on blockchain integration in public procurement domestically, they are also facilitating discourses to foster updates and expansion in blockchain capability-funded programs, with an emphasis on transparency, accountability, and inclusiveness (OECD, 2019; World Bank, 2020).

In addition, multi-level governance structures provide adaptive regulatory approaches to encourage blockchain technology as jurisdictions could choose to make their actual regulations or regulatory frameworks more porous to innovation by using pilot programs or regulatory sandbox principles while using feedback and iteration to manage risk through regulation (Sabel & Zeitlin, 2012). For example, in Canada, the federal and provincial governments have created innovation hubs to experiment with blockchain applications and other technologies to provide public services, such as a procurement program (Government of Canada, 2020). For instance, in the macro-regulatory approach in the USA, individual agencies are maximizing decentralized experimentation; specifically, to encourage collaboration and innovation among agencies.

Still, practicing multi-level governance would require coordination and dispute resolution capabilities to mitigate fragmentation. Fragmentation can result in duplicated effort, inconsistent policies, and conflicts in regulations or laws among institutional actors which can decrease the trust of stakeholders and slow technology adoption. A multi-level coordination mechanism of fluid dialogue, joined technical standards of interoperability, and shared governance protocols for managing the structures of blockchain systems for procurement would help to navigate the complexities of instances of blockchain-enabled procurement systems (Peters, 2015). Additionally, the processes of establishing governance frameworks need to be transparent and inclusive so that marginalized actors of society, including civil society actors, have a voice in the way blockchain systems are adapted, standard for legitimacy in democracy (Bovaird & Löffler, 2016).

In summary, multi-level governance can both complicate and facilitate the process of harmonizing blockchain into public procurement systems. While there are potential intricate challenges presented by overlapping regulatory authorities and legal risks associated with the divergence of legal traditions, supranational coordination, intergovernmental coordination, regulatory experimentalism, and ongoing adaptive regulation offer avenues between states engaging in harmonized sustainable blockchain cooperation. A deeper understanding of these complex governance dynamics can help inform not only the design of blockchain interventions that are both legally compliant and institutionally feasible but also take advantage of its anti-corruption potential as it relates to diverse jurisdictions.

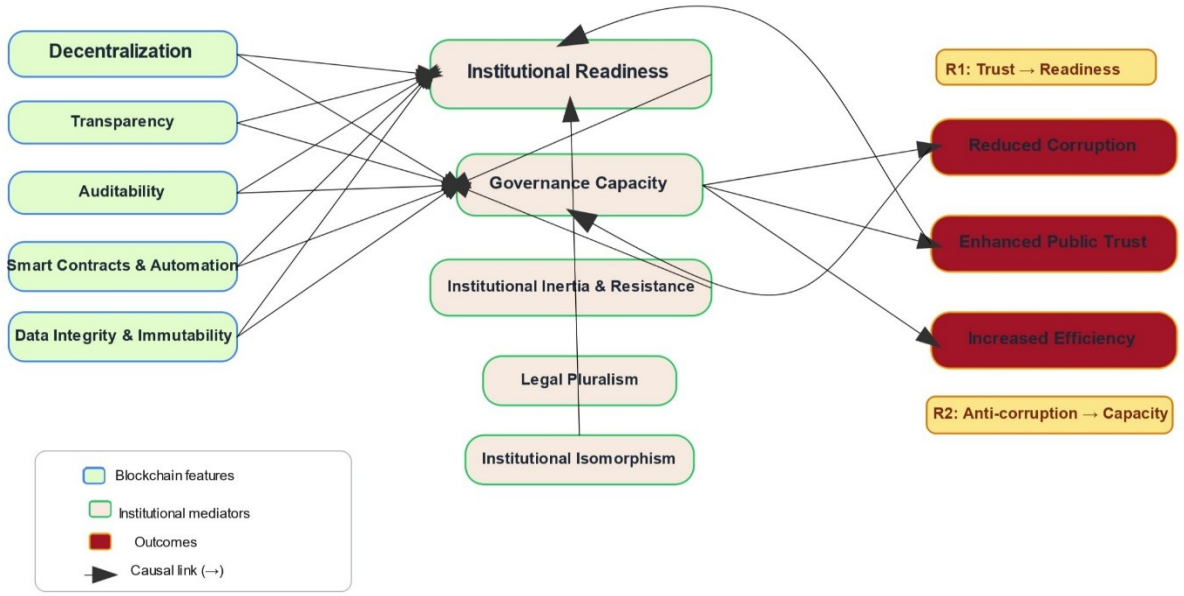

Figure 1.Figure Socio-Technical Causal-Loop Model of Blockchain-Enabled Procurement Integrity (ST-CLM-BPI).

Figure 1. Socio-Technical Causal-Loop Model of Blockchain-Enabled Procurement Integrity (ST-CLM-BPI).

Note. Blue nodes = blockchain features; green = institutional mediators; orange = outcomes. Node size reflects theorized salience (Readiness ≥ Capacity > Inertia/Resistance > Legal Pluralism > Isomorphism). Dashed orange links indicate reinforcing feedbacks **R1** (Public Trust ⇄ Governance Capacity) and **R2** (Reduced Corruption → Transparency/Auditability → Capacity → further Corruption reduction).

The proposed model represents blockchain-enabled integrity in public procurement as a dynamic, socio-technical system in which technological affordances interact with institutional conditions to yield governance outcomes. Rather than a linear input–output chain where fundraising or grant writing is the trigger, the figure captures a network of causal relations with reinforcing feedbacks that are endogenized over time, consistent with systems thinking and system dynamics, where feedbacks govern behavior, not event sequences (Sterman, 2000). On the left-hand side, five canonical properties of distributed-ledger infrastructures—decentralization, transparency, auditability, smart-contract automation, and data integrity/immutability—are treated as exogenous (as opposed to endogenous) technological drivers. At the center, five institutional constructs—Institutional Readiness, Governance Capacity, Institutional Inertia and Resistance, Legas Pluralism, and Institutional Isomorphism—mediate and moderate how the tech-commence drivers are able to be absorbed and subsequently translated into practice. Finally, on the right-hand side, the systems performance is captured in three salient policy outcomes: reduced corruption risk,

increased public trust, and increases in administrative efficiency. The diagram captures two virtuous feedback loops whereby the first refers to R1 (a mutually reinforcing relation between public trust and governance capacity) and the second refers to R2 (a reinforcement sequence whereby reduced levels of corruption allow for increased levels of transparency and audibility which strengthens governance capacity which in turn further reduces levels of corruption), which is consistent with the expectation that governance reforms acting on a technical solution have the potential to generate self-sustaining increases in both capability and legitimacy (Kooiman, 2003; Rhodes, 2007).

In terms of structure, decentralization is viewed as foundational , as it effectively redistributes control over creating and validating records, thereby limiting one-point discretion during sensitive procurement stages (e.g. tender design, bid evaluation, change orders).Its effect is ultimately indirect; through new skillsets, standards in the processing of the procurement, and inter-agency coordination of decentralized systems, institutional readiness and governance capacity are enhanced rather than achieving its desired effect (Narayanan et al., 2016; OECD, 2020).

Transparency and auditability are essentially the types of information transparency (ex-ante) and auditability (ex-post) as they are complementary in nature; where transparency enhances ex-ante verifiability, auditability preserves immutable time-stamped trails that can be verified ex-post. The impacts they 'realize' are dependent on readiness (e.g. data governance, role-based access processes, and existing SOC processes) and capacity (e.g. investigative data analytics and credibility of sanctions) (Meijer, 2013; OECD, 2016, 2020). Smart contracts and automation effectively reduce a routine and discretionary series of micro-decisions through codified deterministic rules where the benefits are conditional on institutional preparedness and willingness to formalize the procurement logic as well as manage exceptions (i.e., ultimately the human factors) (Werbach & Cornell, 2017). On the role of data integrity and immutability, even though they provide evidential verifiability quality that supports and underwrites the other affordances by raising the costs to tamper, they only offer effective protection if the institutions are structured to detect and respond when actors deviate (Narayanan et al., 2016; Finck, 2019).

Of the mediating factors Institutional Readiness is positioned firstly as it represents the sum of conditions necessary to assimilate fundamental institutional factors (e.g., digital infrastructure, master-data quality, skills of staff, standard operating procedures and compliance culture). In developing and mature digital-government contexts, readiness is always associated with effective technology assimilation and consequential gains in performance (Rogers, 2003; OECD, 2022; Zhang et al., 2022).Governance Capacity captures the capacity to design, enforce and adapt rules, to understand blockchain evidence, and establish coherent collaboration across agencies, audit bodies, and courts—all of which incorporate particular forms of technical signals into credible accountability and observable results (Kooiman, 2003; Rhodes, 2007).The model represents readiness and capacity as reciprocal: an early deployment raises procedural literacy and analytic ability, which may allow for more ambitious deployments, governed better, consistent with capability-accumulation processes in public organizations (Mergel, 2016). Institutional Inertia and

Resistance function as a dampening mechanism, reducing the translation of readiness into capacity and outcomes in situations characterized by vested interests, path dependence, or risk aversion (Mahoney & Thelen, 2010). As such, the model indicates weakening effects of inertia and resistance on the central pathways to outcomes - and implicitly on the readiness-capacity relationship - to resemble the non-monotonic effects of technology under contestation (Bovaird & Löffler, 2016). Legal Pluralism constrains the effective scope of smart contracts, and data publishing, delimiting what may be automated or published across overlapping regimes (e.g., EU data protection rights, national procurement codes, sector-specific dispositions) (Berman, 2007; Finck, 2019; Teubner, 1997). Institutional Isomorphism represents legitimacy pressures to replicate peer jurisdictions; while it may accelerate diffusion, its causal leverage on corruption risk is limited where there is no actual capability and enforceable rules (DiMaggio & Powell, 1983; Mergel, 2016).

The outputs are spelled out as measurable governance effects. Reduced corruption is operationalized as a reduction in red-flag indicators in the procurement lifecycle (e.g., single-bid tenders, short calling periods, an excessive number of amendments, winner rotation); these indicators are consistent with existing integrity guidance (OECD, 2016). Improved trust in government is a perceptual construction, likely to be responsive to observable transparency and credible enforcement; the extent of public trust can be proxied by survey evidence, complaints, and breadth of participation (OECD, 2020, 2022). Increased efficiency is defined as shorter cycle times, lower transaction costs, and fewer post-award disputes, which can be evaluated by using process analytics such as time-to-contract, frequency of variation orders, and amount of payment delays (OECD, 2020). The model lets us indicate that each outcome is a joint dependency on readiness (the completeness, timeliness and quality of data) and capacity (the agency's use of that data to monitor, manage and discipline).

The feedback looping component renders the system a path-dependent, dynamic system. R1 states that observing integrity gains for the public, in addition to officials' belief that the rules are being followed increases commitment to a mandate, fosters trust among stakeholders and will therefore justify resources to improve infrastructure and data stewardship and training, which in turn will improve Institutional Readiness, leading to subsequent waves of reform (Rhodes, 2007; OECD, 2022). R2 states that reducing corruption creates opportunities for trust to increase accountability and mandate on the part of the oversight organization to develop further analytic tools, refine the rules and automate the data collection within Governance Capacity, leading to further opportunities to eliminate corrupt influence (Kooiman, 2003; OECD, 2016). Together these loops will help us understand how even early wins that are well-governed are able to create a virtuous path-dependent trajectory, while those being undertaken in a less than genuine manner or as a pilot project, may stall capabilities and damage trust (Mergel, 2016; Mahoney & Thelen, 2010).

The model explicitly indicates that it can be falsified and estimated, and each construct can be operationalized with multi-item, multi-source assessments to evaluate the reliability (internal consistency, test–retest) and validity (content, convergent, discriminant) of each construct. Indirect

indicators of readiness include audited IT-governance scores, data completeness/latency, and certification rates for personnel; capacity indicators include non-OT individual oversight staffing indicate; sanction execution mass; and pace of rule update; inertia indicators include time lag one-use, time lag second time use (second), times policy exception is overridden for bad actors; and legal plurality to deal with dual layer of pervasive constraints is an index; when organizations to adopt, isomorphic process templates has another index common with situation connected across government organizations (OECD, 2020, 2022; Mergel, 2016). Reasonably-identifying the relationships in the calculator requires structural equation modelling or some types of panel estimators or with unit and time effects which can identify contemporaneous pathways (Bollen, 1989). The feedbacks also support time-designs—including cross-lagged panel models (and where wise pre-registered instrumental variables for exogenous events like staged mandated by law to use) or small simulations of system dynamics designed for small scale measurement of the structures based on the process indicators (Sterman, 2000; Angrist & Pischke, 2009; Little, 2013). This method generally follows the causal logic presented in the previous diagram and retains learning and capability's temporality.

this model addresses endogeneity directly. The outcomes directly affect the mediators. Simple regressions suffer from upward bias, but through their lagged structure and external instruments, they avoid bias--(Angrist & Pischke 2009; Little, 2013). Partially due to measurement error--especially for perceptual constructs of trust--they reduce error by matching the administrative traces (e.g., volumes in complaints, participation) in relation to each survey indicator. Common Method Bias--they mitigate by using the system logs for the inputs--they used the outcomes from a separate registry; robust checks used other definitions of red flags (OECD 2016 2020).

Substantively, the model provides reasons for why technology on their own cannot provide the adequate reforms for integrity, or which decentralization does but in non-determinate terms. Though decentralization allowed less unilateral adaptability, without data governance, actionable process rules and sufficient means to account for oversight, discretion means any scope shift is to private opaque actors from traditional public servants (Finck, 2020; Werbach & Cornell, 2017). The framework provides policy levers for implementation from the technology features within both readiness and capacity, and understanding the dampening factors; foundational data investment and process investment where the binding constraint is readiness; investment in analytics and credible sanctions where capability is bottlenecked; change management over inertia, targeting harmonization or exception strategies where legal plurality impedes automation (OECD, 2016, 2020, 2022). Lastly, the feedbacks continue to inform sequencing: first, they can begin activating transparency initiatives to produce early R1, whilst managing the level of commitment scaling by also supervising the translation of any discouragement identified with select levels of enforcement in the most consequential segments to trigger the R2--over time cumulative causation would broadly agree with how their model works (Mergel, 2016; Rhodes, 2007; Sterman, 2000).

3.4. Research Methodology

3.4.1. Research Design: Multi-Modal Document-Based Comparative Analysis

In this dissertation, a multi-modal document-based comparative analysis is selected as the overarching format of the research design, which effectively synthesizes qualitative legal–institutional document analysis with a directed descriptive quantitative module. The intent is to produce a systematic examination of how the integration of blockchain technologies are framed, regulated, and acted upon in the area of public procurement reform and anti-corruption governance in three national jurisdictions: Italy, Canada, and the United States. This research design has its methodological orientations in established traditions of legal–regulatory analysis and inquiry, comparative institutional analysis, and technology governance studies.

The rationale for this design can be viewed through both epistemological orientation and empirical limitation. Given the overlapping complexities of legal systems across multiple jurisdictions and the normative nature of many policy processes, a document-based strategy allows the researcher to engage directly with texts of authority as well as regulatory frameworks, pilot reports and institutional strategies. Document analysis lends itself to explicitly treating governance documents as intentional artifacts that represent formal commitments and administrative constraints. A document-based design is particularly appropriate to advancing the procedural, structural, and discursive aspects of blockchain integration in public systems that is inherently uncertain (legally and technologically) and experimental (technologically and policy-wise).

The research design is developed across two complementary sections. The qualitative core is based upon the structured analysis of public documents categorized by legal–regulatory and technology domains. The data analysis entailed thematic and content analysis to organize patterns, trace the evolution of policy formation, and map the gradual introduction of blockchain mechanisms against corruption typologies and stages in the procurement lifecycle. The second extension is prompted by the introduction of a descriptive quantitative component, to further support the interpretive framework and more broadly contribute to macro comparisons. Governance indicators – specifically the Corruption Perceptions Index (CPI), World Bank Control of Corruption scores, and procurement digitization metrics – provide context to the document's findings and also contrast the jurisdictional differences in institutions' readiness and capacity against corruption.

Subsection 4.1.1 elucidates the rationale for employing a document-based comparison technique, asserting its appropriateness for legally oriented, multi-jurisdictional research and its congruence with the structural attributes of the study domain. The mixed-method typology of the study is

reframed in subsection 4.1.2, to clarify that the aggregation of quantitative indicators serves distinct interpretive and contextual task rather than statistical function of analysis. These methodological choices act together to form a cohesive and scientifically rigorous design that appropriately balances depth and comparability to demonstrated analytical validity and policy significance to the dissertation.

3.4.1.1Justification for Document-Based Comparative Methodology

The decision to use a document-based comparative research design stems from a combination of practical limitations and conceptual opportunities related to the study of legal, regulatory, or technological structures and systems across jurisdictions. There are clear structural limitations on original primary data collection (limited access to the relevant institutional actors, legal confidentiality limits, and spatial constraints of key stakeholders), thus document-based classificatory frameworks represent a practical and rigorous alternative to examine institutional processes and normative mechanisms. Document-based approaches are particularly useful in cases where some form of public data is required by law, such as procurement law or related to governance through transparency laws, endowing a document-based strategy with some practical regulatory legitimacy as well as reliability as a source of evidence.

Methodologically, for studies transcending across legal systems, governance frameworks, and new modes of digital governance, document-based analysis affords researchers the ability to have continuous access to data bound by time, type, and procedure. Document-based approaches offer researchers access to written material that is historically bound, institutionally grounded, experiential, and was not necessarily influenced by respondent biases or retroactive rationalizations. Legal documents, regulatory instruments, compliance reports, and technical documents prepared by governmental agencies articulate the state's formal position, legislative intent, and codified procedure. These constructs are central to a study that is examining how different jurisdictions are framing, regulating, and resisting blockchain technologies. When researchers analyze and compare these textual artifacts, the nature of each is bound by its role in institutional logics constants that researchers can capture across settings. Assessing the processes captured in this document-based design allows for rich comparisons across civil (Italy), common law (Canada/United States), and hybrid legal systems. In addition, document-based approaches reflect existing practices in legal-technical research when doctrinal exegesis is paired with an empirical examination of public policy. In domains where the implementation of new technologies intersects with compliance obligations, a careful examination of pilot project documents, technical specifications and white papers, is necessary to unpack how these technologies are framed, governed and operationalized. This is particularly prevalent in the blockchain space, where the discourse around notions like immutability, interoperability and algorithmic accountability often rely upon institutional and regulatory language.

In terms of cross-jurisdictional comparison, document-based methods can facilitate a systematic capture of the convergence and divergence between national systems. Legal and policy

documentation can serve as reflections of national capacity, institutional readiness and policy direction. It is also worthwhile to note that the paper trail facilitates an investigation of national documents as they change over a five-year period, a period that marks the time of the global rise of blockchain in public sector innovation. The paper trail is necessary to enable a purely vertical analysis of developments, which is to observe the progression of material in the same jurisdiction over time, as well as a horizontal analysis of the changes over time in other jurisdictions at the same time. This temporal-spatial mapping is critical to the aims of the thesis which aims to identify aspects of anti-corruption regulatory mechanisms and innovation dissemination through the deployment of blockchain.

Finally, to parallel the document-based qualitative component with a descriptive quantitative element adds a layer of value in this design. By supplementing macro-scale descriptors such as the Corruption Perceptions Index (CPI) from Transparency International, World Bank governance assessments and e-procurement transparency metrics of States, I am able to contextualize my document products with country-level empirical data. This also validates my interpretive analysis because it anchors the document interpretations within observable dynamics pertaining to countries. These measures should not be considered inferential, but rather contextual layers that can stimulate the depth and relevance of my analyses of the documents. Thus, my project benefits from a methodology that is multi-modal, rigorous from ana

analytical perspectives and contextual from the aspects of jurisdictional variation, uniqueness and complexity.

3.4.1.2Reframed Mixed-Method Typology

The methodological framework of this dissertation represents a conscious remapping of traditional mixed methods approaches. Rather than adopting a "qualitative-dominant" framework, which is common in interpretative legal or governance studies, the design is better characterized as a document-based comparative analysis with an strategically bounded quantitative module. This remapping is more than a change in vocabulary. It evidences a fundamental readjustment in the epistemological foundations of the study with respect to both the nature of the study-specific research questions (and why they are important), as well as the type of data to be collected, and the jurisdictional heterogeneity of the phenomena of interest.

In traditional mixed-method designs, the merging of qualitative and quantitative approaches overlap with together through the sequential or concurrent imbrication of facets such as interviews, surveys, and statistical testing. However, these models are not well-suited to normative documents, regulatory instruments, and technologically-specific state publications. It is from this standpoint that this research's epistemic strategy is predicated on systematic document analysis- using formal legal, regulatory, and technologically artifacts as the principal units of analysis. These documents

are not simply narratives written by the state, but instruments of governance that encode institutional intent, policy rationales, and regulatory constraints.

The qualitative facet of this study is deeply engaged with these documentary sources, through thematic or content analysis, structuring its findings in part through deductive coding (with respect to corruption actor typologies and blockchain-specific instruments for governance mechanisms), and in larger part, through inductive reasoning (with respect to patterns emerging from document corpora).The analysis treats legal statutes and regulatory frameworks, as well as technological pilot reports, as systematic discursive forms, thereby enabling grounded interpretation across both the normative intent and logic of practice.

At the same time, the addition of a descriptive quantitative component serves two important purposes. First, it affords empirical grounding to the document analyses by situating country-specific discourse within broader macro-level governance trends. Second, it enriches the explanatory capacity of the qualitative findings by offering a baseline of comparative performance indicators—levels of perceived corruption, procurement transparency, and institutional trust among others. Again, these indicators are not to test hypotheses or generalize statistically, but to record the structural conditions under which blockchain technologies are being adopted—or resisted—by national public procurement systems. In this sense, the mixed-method typology that has been configured retains methodological coherence, while at the same time allowing for flexibility across different data types. Most significantly, the descriptive quantitative module does not act as a parallel analysis stream, but rather as a layered interpretive scaffold that supports and enhances the documentary core. This layered architecture—qualitative analysis of structured documents, plus providing contextual evidence using empirically validated governance indicators—ensures both analytical depth and comparative insight.

The decision to adopt this methodological hybridization was also shaped by the epistemological demands of cross-jurisdictional analysis. Comparative legal–regulatory studies can be complicated by structural differences in legal traditions, administrative cultures and public sector innovation capacity. A fully qualitative and fully quantitative approach would risk subscribing to overly reductive interpretations of these contextual realities. In contrast, the selected document-based design, supplemented by thoughtful empirical indicators, sustains the legitimacy of jurisdictionally focused meanings while delivering calibrated cross-case levels of insight.

Furthermore, the reframed typology adheres to established practices in mixed-methods jurisprudence and policy studies, where methodological pluralism is both acceptable and encouraged to address multi-scalar governance challenges. Creswell and Plano Clark (2018) describe that "the real advantage of a mixed-method design study is the ability to use the strengths of one method to purge the weaknesses of another" (p. 153). In this case, the qualitative document analysis, provides granularity, specificity of legal references and meaning, and interpretive richness, while the descriptive quantitative module offers external validity, cross-case comparability, and macro-level orientation. This provides coherence and relevance to the study.

Practically, the reframed typology undergirds all aspects of the study. The document selection and coding (Section 4.2) processes follow protocols based in qualitative content or thematic analysis and the quantitative data are derived exclusively from internationally recognized data sources such as Transparency International, the World Bank, and national procuring portals, undergoing basic descriptive analysis (see Section 4.3.2) to create outputs such as mean CPI scores, procurement digitization rates, and e-GP platform usage trends subsequently used as an interpretive—not statistical—layer of triangulation, reinforcement, or a challenge to patterns from the document analysis.

In short, this reframed mixed-methods approach creates a methodologically strong and context-sensitive design for legal–technology anti-corruption research which achieves the destination of preserving the depth of quantifiable document-based inquiry, while embedding that inquiry within a larger set of empirical support that adds to comparability. This dual layered position (of design and approach) is critical for answering the central dissertation question for legal–technological anti-corruption research regarding their feasibility, regulatory context, and capacity for anti-corruption across Italy, Canada, and the United States.

3.4.2 Data Collection Methods: Deepening Document Analysis

3.4.2.1 Primary Data Source: Systematic Document Analysis

Due to the interdisciplinary and jurisdictional comparative nature of this dissertation, the principal method for collecting primary data relies on a systematic document analysis of legal, regulatory, and technical documents. This method is based on standard qualitative research traditions that regard documents as purposeful, ordered, and communicative accounts of institutional action (Bowen, 2009; Prior, 2011). The purpose of the document analysis is to facilitate an understanding about how public procurement, anti-corruption frameworks, and blockchain-related policies become articulated, debated, and mobilized across three legal systems: Italy, Canada, and the U.S.

The primary rationale for focusing on official documents in lieu of primary interviews or observations is twofold. First, legal and policy documents are authoritative expressions of the state's regulatory intentions and administrative directions. In nascent fields such as public procurement and digital innovation governance, the document(s) does not simply represent a story, but the document is constitutive of the legal terrain where technologies such as blockchain or digital legislation may be adopted or not adopted. Second, documents frequently come pre-loaded with empirical content (e.g., pilot project evaluations, implementation reports, regulatory impact assessments), which provide analytically rich material that goes beyond the influence of law and legal analysis.

The types of documents that are included in this study are purposefully broad even in the context of publicly funded engagement; this is done to match the multi-level and multi-actor character of the governance of public procurement. The corpus of documents consists of: Legal sources include national procurement codes, (for example, Codice dei Contratti Pubblici in Italy), secondly-

specific legislation, administrative case law and constitutional provisions pertaining to transparency and data protection.

Regulatory sources include guidelines issued by oversight authorities (for example, ANAC, Treasury Board of Canada Secretariat, Office of Federal Procurement Policy), government innovation strategies, and compliance monitoring reports. Technical or pilot reports produced by state agencies or intergovernmental consortia, which assess the implementation of blockchain (or related technologies) into public procurement ecosystems. Academic and institutional publications produced by organizations including the OECD, World Bank, EU Commission, as well as peer-reviewed journals, that analyze the feasibility, design logic and implications of blockchain governance for public sector contexts. The documents are included for their legal relevance, jurisdictional specificity, and evidentiary accordance with the research questions, not to simply increase the sample size. A structured search protocol is included in the following pages to provide methodological transparency.

The procedure to identify documents followed a systematic and replicable search strategy across the various jurisdictions and institutional sources. Search terms were designed to reflect the thematic scope of the dissertation and included combinations of keywords: blockchain, public procurement, transparency, smart contracts, digital government, anti-corruption, and regulatory frameworks. These search terms were applied to selected databases, including the official government websites (for example, ANAC, Gazzetta Ufficiale, Canada.ca, U.S. The Federal Register, international institutional repositories (e.g., OECD library, World Bank Documents), and legal research databases (e.g., LexisNexis, CanLII, EUR-Lex, and HeinOnline) were used as data sources. Searches were conducted in both English and local legal languages (Italian or French when applicable) to increase jurisdictional accuracy and comprehensiveness.

Documents were selected from these sources based on a rigorous set of inclusion and exclusion criteria. The inclusion criteria included: (1) formal legal/logical relevance, (2) clear jurisdictional identification (Italy, Canada, or the United States), (3) direct engagement with blockchain, procurement or anti-corruption policy topics, and (4) publication date of 2015-2025, this period matches the institutional arrival of blockchain in governance related to public procurement and anti-corruption. Documents were excluded if they were (a) promotional in nature for commercial purposes, (b) repetitive or superseded in regard to other recent documents, and/or (c) not research-informed or analytical. When appropriate, cross-referencing techniques were used to track document lineage and validity—for example, verifying if reports cited were adopted as policy, published as drafts, or withdrawn.

To ensure analytic consistency and auditability a comprehensive document control sheet (metadata matrix) was developed and maintained throughout the data collection phase. The metadata matrix

recorded the following fields of data for each document source jurisdiction, issuing authority, publication year, document type (e.g., specific forms of legal, regulatory, technological, academic), institutional provenance, and topical keywords. The metadata matrix was managed in Excel for tabular control and then imported into NVivo for qualitative coding, indexing, and cross jurisdictional retrieval. This supported iterative theme generation and conducting structured comparisons and easy tracking for evolving patterns in the analysis phase.

By merging methodological rigor in document retrieval with structured metadata coding and thematic indexing for the data repository, the research provides high confidence that the primary data corpus is scientifically valid and analytically tractable. This follows best practice in qualitative legal–policy research, particularly in transnational regulatory analysis when institutional complexity demands systematic treatment of documentary sources (Scott & Raj-Reichert, 2020).

3.4.2.2 Secondary Data Source: Descriptive Quantitative Module

Although the primary analytical emphasis of this dissertation is on the interpretation of legal and institutional documents, it also has a secondary descriptive quantitative module to enrich and provide context to those findings. The module is not for causal inference or hypothesis-testing, but simply as a descriptive empirical backdrop in which the legal - regulatory dynamics of blockchain adoption in public procurement can be placed. It also offers the study the ability to frame the qualitative findings within measurable cross-national trends by the inclusion of governance and transparency indicators at the macro level.

The quantitative data are drawn from globally respected and rigorously sourced data repositories, thereby ensuring both reliability and comparability across countries. The most significant of these is the Corruption Perceptions Index (CPI) published by Transparency International, which reports on the perceived levels of corruption in the public sector across 180 countries, as an annual score. The CPI is frequently referred to both in the literature surrounding academics and policy, as a proxy for the integrity of institutions, and is particularly relevant in this study because it will also facilitate the evaluation of anti-corruption across procurement. In particular, this measure allows for the study to compare exposer risk environments in Italy, Canada, and the United States during the 2015-2025 period.

The other comparative element is the Worldwide Governance Indicators (WGI) dataset compiled by the World Bank, which captures six general dimensions of governance: voice and accountability; political stability; government effectiveness; regulatory quality; rule of law; and control of corruption. This dissertation emphasizes the dimensions of "control of corruption" and "government effectiveness" because they dictate the institutional conditions through which blockchain policies are conceived and executed.

Procurement-specific data are also included from the Open Contracting Partnership (OCP) and relevant national e-procurement portals, so that data related to rates of publication of contracts, vendor engagement, tender transparency, and digitization of the procurement workflow can be

analyzed. For example, in Italy, the ANAC open data portal provides indicators related to awarding contracts and corruption red flags. In Canada, Public Services and Procurement Canada (PSPC) and the Buyandsell.gc.ca portal provide data indicators related to electronic tendering and supplier diversity. In the United States, procurement indicators are sourced from USAspending.gov and the Federal Procurement Data System (FPDS), which provide detailed transaction records.

This suite of indicators was selected not simply for their empirical value, but for their potential to shed light on structural preconditions and contextual restrictions that inform the legal and technological adoption patterns of blockchain systems in procurement practices.

The analytical use of these indicators is fundamentally integrative, not disparate or, perhaps, unrelated. Their primary purpose is to provide context to the document-based findings by situating country-level legal and policy developments into empirically observable governance contexts. As an illustrative example, if a jurisdiction exhibits comparably high CPI scores (which suggests low levels of perceived corruption), in conjunction with advanced levels of procurement digitization, this fact can then be analytically compared with that jurisdiction's, ontology of regulatory openness toward blockchain use. Low levels of governance scores on the other hand may signal a more fragmented or hesitant regulatory posture, thus allowing for hypothesis-informed interpretation in the analyzable comparative legal context.

Significantly, the descriptive data are not analyzed for inferential statistics or regression analysis, but instead summary metrics, including annual means, directional trends, and comparative rankings are used in visually represented (e.g., line graphs, bar charts, comparisons of countries in tables) and to support the qualitative interpretive analysis of coherence in policy, institutional readiness and capacity for anti-corruption. Exceeding the evidentiary epistemological status of quantitative, the descriptive information is intended to substantively reinforce the analysis of the core document analysis.

The use of descriptive data in quantitative analysis has another function as well, when utilized by ontological triangulation in a research design. Specifically, the applications of thematic findings, in terms of policy and legal texts, to macro-governance indicators concurrently, increase internal credibility and external plausibility associated with triangulation. For example, regulatory documents from Canada set out aspirations towards transparency in procurement, or for that matter the adoption of innovation, for those provisions can be contextualized and subsequently verified with upwards trends shown in relevant macro-governance indicators, alongside procurement digitization metrics. In other words, to strengthen conceptualizations and logically more robust contextual understandings - especially with terms/claims made in a document or interpretation that is aspirational, as opposed to strategic, language will depend on contextualizing the overall governing dynamic represented through purchasing.

Finally, in conjunction - this quantitative module works in part to allow comparability between jurisdictions by providing a standardized lens to compare national differences in a meaningful way. Outside of legal frameworks that uniformly the law in operation across Italy, Canada, and the

United States, comparative metrics in governance (somewhat) offer a baseline analytical lens to sort and analyze idiosyncratic language of national law from systemic attributes of a governance framework that provide comparative validity to a framework.

In sum, the descriptive quantitative component does not reduce or dilute the legal and institutional richness of the document analysis. Rather, it positively affirms more robust interpretive research, comparative depth and contextual credibility of a mixed methods research design. This is but one initial example of many that confirms the merits of multi-modal prescriptive re-join a research design aimed at complex, multi-jurisdictional governance inquiry.

3.4.3. Data Analysis Methods

3.4.3.1.Qualitative Analysis of Documents

The central analytical method applied within this research is a qualitative analysis of legal, regulatory, and institutional documents that is structured. This methodological approach is predicated on the epistemological assumption that documentary artifacts are not passive records but rather active mechanisms of governance, communication, and the influence of policy (Prior, 2003; Bowen, 2009). Documents are seen as purposefully constructed, politically-located artifacts produced by institutional actors and can thus be considered analytically rich sites for the construction of meaning. The qualitative analysis is meant to reveal the patterns of themes, discursive logics, and institutional signals found within the documents, specifically the theme of blockchain technology in relation to public procurement and anti-corruption governance in the jurisdictions of Italy, Canada, and the USA.

The primary method used is a deeply thematic analysis defined around a nested, iterative, multi-stage coding scheme. The analytical process adapted Braun and Clarke's (2006) thematic model and had six stages: (1) familiarization with the text of each document through repeated close reading; (2) generation of initial codes that reflect prominent policy concepts, legal provisions, and technical language; (3) identification of both latent themes and semantic themes; (4) iterative merging and refining themes into interpretive categories; (5) assembling jurisdiction-specific and cross-jurisdictional matrices; and (6) interpreting themes within the overall research framework. This was a method of qualitative analysis that facilitated both vertical (within-jurisdiction) and horizontal (cross-jurisdictional) pattern recognition.

The coding process leveraged deductive and inductive logics. The organization of the coding scheme was both deductively and inductively informed. Deductively, it was informed, initially, by the theoretical framework of the dissertation, specifically by typologies of corruption actors (e.g., state capture, collusion in procurement, and opacity of the administrative process) and known mechanisms of governance in blockchain (e.g., immutability, automation of smart contracts, and auditability). The theoretical categories guided the initial structure of the coding scheme and allowed the empirical data analysis to align with the conceptual structure of the dissertation. Inductively, through the process of coding, additional codes were allowed to emerge directly from

the documents, especially, but not exclusively, in relation to constraints or impediments linked to the jurisdiction (e.g., legacy systems and legal uncertainty) and discursive strategies (e.g., aspirational or risk-hedging language in evaluations of pilot projects).

NVivo was used as the main software platform to manage the corpus of documents, to apply the coding scheme, and to create visual displays of the quantitative data that included code frequency distributions, thematic co-occurrence matrices, or comparison charts organized by jurisdiction. This was all done in the interest of transparency, auditability, and analytical traceability within the data analysis process.

Along with the thematic analysis, a secondary content analysis was conducted to provide quantitative support for the qualitative findings, by measuring the frequency (and distribution) and contextual use of specific key terms that either described legal–technical discourse or related to corruption prevention (e.g., immutability, interoperability, smart contract, compliance, transparency). The lexical analysis permitted the analysis of institutional emphasis across jurisdictions and types of documents, rhetoric framing, and policy orientation. For example, references to immutability in Italian regulatory discourse were often accompanied by cautionary qualified language referring to the legal revertability of contracts under civil law, whereas Canadian documents emphasized interoperability as a feature of platform governance and federal–provincial coordination. Such content mapping facilitated a greater understanding of the narrative framing strategies employed by each jurisdiction. A comparative jurisdictional analysis was subsequently undertaken to synthesize patterns across legal traditions and administrative cultures. This included the development of structured matrices comparing how blockchain technologies were legally defined, procedurally embedded, and discursively contested across Italy, Canada, and the United States. The comparative perspective revealed significant divergences, for example, differences in the level of legal recognition of smart contracts, as well as significant similarities, such as a common focus on transparency and auditability as anti-corruption enablers. Further, the analysis integrated elements of adaptive learning and policy transfer, examining whether and how jurisdictions referenced or responded to developments in peer countries or supranational organizations as part of the analysis. Additionally, the analysis involved a relational mapping of blockchain governance mechanisms onto actor-specific corruption risks outlined in Section 2.1.2. For example, blockchain's auditability function was often related to the alleviation of bid-rigging and post-award opacity, while smart contracts were considered a mechanism to reduce discretionary manipulation in contract execution. Relational mapping was not imposed a priori, but was drawn from the institutional language and deployment logic employed in government pilot reports, government legal memoranda, and assessments of blockchain applications. The link between technological affordances, the legitimacy of specific corruption risk types, and the potential of blockchain systems to address such risks represented a significant connection in order to conceptually examine their practical anti-corruption applicability in public procurement.

The combined use of thematic, content and comparative analysis provided a multi-dimensional interpretation of the various documents. This combination helped advance the analysis from basic

description to the identification of institutional rationalities, normative contexts, and jurisdictional constraints that shape the discourse and practice of blockchain-based governance. Overall, this combination of data prompted a multi-layered analysis which bolstered methodological rigor while responding to the complexity of the legal–technological research context.

3.4.3.2. Quantitative Data Analysis (Descriptive)

This descriptive quantitative aspect of the study plays a supporting role relative to the overall analytical framework. Unlike inferential, or predictive statistics, which seek to generate causation or generalizability, this piece is limited to description statistical methods that serve to contextualize the qualitative document analysis with observable empirical trends. The aim is to provide a macro-level context of governance, transparency, and corruption variables in ways that enrich the interpretation and comparison of the legal–regulatory analysis. The analytical approach began with the systematic layering of annual indicators from internationally standardized datasets. The included indicators were sourced from datasets such as Transparency International's Corruption Perceptions Index (CPI), the World Bank's Worldwide Governance Indicators (WGI), and procurement-oriented datasets from Open Contracting Data Standard (OCDS), ANAC (Italy), Buyandsell.gc.ca (Canada), and Federal Procurement Data System (U.S.). Each of the indicators was selected based on methodological legitimacy, the ability to be compared across countries, and direct relevance to public procurement governance. To ensure analytical consistency, data were normalized on a comparable scale, as index scores (0–100), percentile ranks, or standardized units. For example, CPI values 0–100 scales were used, where higher values indicate lower perceived corruption. WGI control of corruption scores, originally reported in z-scores, were converted to percentiles for ease of interpretability. Metrics on procurement digitization—such as the percentage of electronic publication of public contracts—were operationalized in percentages as field indicators of transparency infrastructure. Basic summary statistics were used to analyze trends over the ten-year period for the study (2015–2025), including measures of central tendency (mean, median), dispersion (standard deviation), and directional difference (year-over-year deltas). For example, the change in CPI scores across years was used to measure if macro-level perceptions of corruption improved or worsened during the investigation of any blockchain piloted procurement reforms. The publications rates of procurement were similarly tracked to see if these publication increases increased transparency uniformly in conjunction with regulatory or technological changes. Descriptive statistics were then categorized by jurisdiction, and analysis was grounded within the thematic connections to findings from the document analysis phase, allowing for internal coherence and interpretive alignment across the multi-modal methodology.

Descriptive statistics were reported using data visualization techniques appropriate for tracking the differences across jurisdictions and over time. This included some combination of line graphs (temporal change), bar charts (category comparison), and stacked area charts (compound indicators that allow for the tracking of procurement digitization elements). Data visualizations were created using Microsoft Excel and, each identified key indicator was examined in various visualizations for clarity in reportable accuracy. Each visualization was not intended to stand

wholly as a finding, but was used as a point context when discussing and representing the theme of each. In the case of Italy, for example, combining a graph of CPI time-series with digitalization rates of procurement by ANAC allowed us to illustrate a visual connection between institutional anti-corruption work and modernization of the mode of procuring. A chart in Canada contrasting government effectiveness scores with mentions of blockchain in procurement documents depicted the connection between administrative capacity and the technological innovation discourse in public policy. In the United States, procurement openness scores from USAspending.gov were used to compare the fragmentation of states with the federal outputs from a blockchain-based pilot project. These visualizations in and of themselves were not overlapping hypotheses or instruments. Rather, they enable triangulation in an interpretive framework, with quantitative summaries substantiating, pushing back challenge, nuance the evolving legal–institutional narrative that was developed through thematic analysis in this dissertation.

Presentation of the metrics is undertaken in a comparative framework, with all three jurisdictions treated in parallel. This allows for diachronic (within-country, across-time) and synchronic (cross-country, across-time) interpretation. Furthermore, presentation occurs with either narrative, the limitations of the data, its bounded interpretability such as potential measurement error, missing values, or misinterpretation of perception-based indicators, e.g. CPI.

Most importantly, all quantitative insights were analytically related to the stated research objectives. For instance, the finding that the rising transparency metrics and blockchain implementation happened as expected was used when bracketing our arguments of technological feasibility and institutional proclivity for the expected argument of timing. Where metrics are stagnant, stagnation is interpreted as potential institutional inertia, regulatory delay, or superficial reform is the expected argument. Thus, the descriptive statistics are not unintended (inter)claims; they are diagnostic variables for assessing and evaluating accord—or discord—between institutional claims and governance reality.

In sum, the analysis of quantitative data provides a highly bounded methodological role for this study, grounded in empirics, as intersubjectively triangulated, and for the comparative coherence of the document-based analysis. … this layered of presentation brings normative legal discourses, measurable institutional recidivism, and the upper bounds of insight together to fulfil the epistemological work of the multi-modal, comparative, nor-for-profit, unobtrusive research outlined.

3.4.4. Research Quality Criteria

3.4.4.1 Trustworthiness and Rigor (Qualitative Dimensions)

In qualitative research, including document-based and interpretive legal studies in particular, validation of findings is not based on statistical generalizability but rather the trustworthiness of the process of analysis. Trustworthiness is a general term for a collection of methodological benchmarks developed to ensure that the interpretations presented in a study are credible,

transparent, and transferrable. This section describes the primary strategies that were used to support rigor in the document analysis portion of the research, referencing widely accepted benchmarks, such as Lincoln and Guba (1985), Yin (2014) and Bowen (2009).

Credibility, is the first dimension of trustworthiness that was established through a process called analytic triangulation. Triangulation in this case means cross-referencing thematic findings across multiple data types, including legal, regulatory, technological, and academic documents, as well as the use of additional empirical data - most notably quantitative indicators. Inferences about themes from government white papers, for example, were confirmed using similar documented regulatory texts or reports from international assessments (i.e., OECD procurement diagnostics). Triangulation serves to increase interpretive plausibility, ensuring that thematic findings do not emerge exclusively from outlier or singular sources. Further, prolonged engagement with the corpus of data (multiple readings and re-coding the data) ensured thematic saturation had occurred and reduced the risk of premature closure or selective coding/interpretation.

The second dimension of trustworthiness was referential adequacy, which was a reflection of the transparency of the citation trail developed throughout the process of analyzing the documents reviewed. Each source was specifically labeled with a discrete document ID in the codebook meta-matrix to allow for each interpretive assertion to be traced back to a specific legal or institutional text. When appropriate (e.g., Italian statutory provisions), citations were retained in their original language, and full text archival copies were saved to a secure repository for audit purposes. This audit trail is an important aspect of methodological transparency in legal–policy research, where accuracy of terms and descriptions of context are important.

The third qualitative rigor criterion reflexivity, was intentionally employed in analysis. Reflexivity is the researcher's critical understanding of their own positionality and interpretive role in analysis. The study, in this analysis component, was particularly concerned with the risks of interpretive bias as a result of the cross-jurisdictional subject, given the differences in legislative language, administrative style, and policy framing. To counteract this concern, debriefing about coding decisions occurred with other legal scholars from each jurisdiction, and analytical memos were used to record shifts in emphasis about themes in detail during the iterative coding process. Together these strategies ensured the interpretive analysis was not unduly influenced by the researcher's own normative position or disciplinary background, which would have led to interpretive bias. Lastly, transferability, a quality of qualitative research, was assured by embedding jurisdiction-specific detail throughout the document analysis process. Rather than abstracting institutional behavior to generalizable categories, the study purposefully retained contextual specificity about each country's legal system, administrative context, and procurement governance processes. Operationalization occurred through the creation of thick description and document annotation—directly linking legal provisions, regulatory provisions, and pilot studies to the associated institutional and policy contexts. This level of detail is necessary for other scholars

to then determine the potential transferability of findings in similar legal-technical contexts, while also establishing robust attestable empirical evidence for a future replication study across cases.

The fifth criteria, dependability, was attended to through formal audit trail describing every decision of process and analysis, or formal documentation of the major decision made in the reading or document selection procedure. In this audit trail, I maintained: (1) version control of my coding frameworks with timestamps, (2) documentation of notes on inclusion and exclusion decisions while documents were selected, (3) a complete catalog for all metadata, and (4) a coding log exported out of NVivo. The audit trail created by the researcher was a best practice for reflecting qualitative research transparency and rigor. This was particularly important for this doctoral study associated with policy analysis, because methodological defensibility is paramount in establishing the scholarly or practical credibility of any research.

Finally, processes and analytical safeguards reinforce the confirmability, or the degree of influence of researcher bias in shaping the study findings in the document-based analysis. All thematic claims are only based on coded excerpts that are traceable to data reference materials. In addition, triangulation of data with descriptively quantitative indicators to inform temporal validity in data analysis also provides some level of independence analytically from the interpretive data analysis. By connecting observed document-based patterns of follow-like conduct to quantitatively measurable governance indicators, such as procurement transparency rates on the Contracting Plains, trends in Corruption Perceptions Index (CPI) performance etc. of two data derived from causative indicators, resist over-interpretation of findings, and maintain the overall. A good proportion of each of the analysis is grounded by inference elsewhere.

Collectively, these six criteria (i.e. credibility, referential adequacy, reflexivity, transferability, dependability, and confirmability) underlie methodological trustworthiness in the qualitative document-based analysis. They ensured the document-based evidence generated in this study is not only texturally-robust in its interpretation but it can also be traced analytically through a theoretical lens and procedurally to the research study. In doing so, this dissertation filled epistemological requirements of the qualitative standard of research associated with public law, regulatory studies, and technology governance analysis.

3.4.4.2Validity and Reliability (Quantitative Dimensions)

Even though the quantitative component of this research is descriptive rather than inferential, valid and reliable measures of the data are important to the integrity and coherency of the document interpretation. With the study being multi-modal in design, quantitative measures supported, rather than hypothesized, qualitative discoveries. Still, the descriptive measures needed to meet some methodological standards of applicability to ensure that they served their intended purpose: to contextualize document-based interpretations and enable cross-jurisdictional comparisons of document-based interpretations.

With regard to validity, the quantitative metrics used in this study adhered to globally accepted and methodologically transparent forms of measurement. One metric, the Corruption Perceptions Index (CPI), comes from a complementary methodology developed by Transparency International that combines expert assessments and business surveys for many of the institutions that develop this composite measure. Generally, the use of the index in, for example, political science, public administration, and policy studies has established some level of construct validity as a measure for institutional corruption. Similarly, the Worldwide Governance Indicators (WGI) developed by the World Bank rely on a methodologically rigorous aggregation process across six aspects of governance and are considered to be credible indicators of macro-institutional performance.

Indicator choices were based on the conceptual fit of the metric and the analysis. Indicator choices were not stakeholders based on data availability; instead, each indicator had to either incorporate one, or a modified version of one of the four analytical topics: transparency, institutional trust, regulatory effectiveness, or digital procurement maturity. As an example, the CPI indicator utilized rates of procurement publication from national e-procurement platforms (ANAC OpenCUP, Buyandsell.gc.ca, or USAspending.gov), which was a logical argument in that for each dollar spent electronically, the us in referring to the procurement publication rates and their clear relations to transparency infrastructure, which was a significantly important topic of blockchain initiative feasibility and its potential for anti-corruption.

To evaluate content and construct validity quantitative indicators were also supported by citations from references within the document corpus. Anytime national reports or white papers used the CPI ranking or procurement openness numbers as corroborating evidence for their justification of employing blockchain, the evidence provided support toward demonstrating conceptual relevance and salience with respect to policy implications. Together, each source of confirmation demonstration of validity, namely from external institutional data set(s) and from primary source document(s), thereby reinforcing the validity of evaluative measures within the broader study.

In achieving reliability, the research adopted sources with stable data collection protocols developed and refined across time and jurisdictions. The CPI and WGI are reported annually using a consistent methodology and are therefore comparable across reporting periods. Procurement datasets, whether from Open Contracting Data Standard (OCDS) datasets or governmental open data portals, typically have pre-defined schema and templated reporting to reduce interpretive variability. Consistency is important to ensure trends in time are not due to a change in measurement rather the source of institutional change.

To maintain measurement reliability, we sourced all raw data from original, verified sources, including satisfactory metadata documentation that outlined definitions, boundaries and limitations. Data cleaning and normalization was done with Excel, each data transformation – including percentile transformation or jurisdiction cross-alignment – was shown in a repeatable trail, necessary to ensure that descriptive visualizations shown in Chapter 5 are methodologically legitimate and repeatable.

In saying this, we recognize there are limitations in cross-national comparative analysis using macro-indicators. First, perception-based measures, like the CPI are widely cited but do not measure actual corruption events based on some perception of selected respondents. Second, data availability varies from jurisdiction to jurisdiction. For example, Canada and the U.S. open high-frequency, disaggregated procurement data with transparent digital procurement platforms, while Italy's datasets are more fragmented and less standardized. Third, some constructs of governance (e.g. trust in digital government; responsiveness of institutions) are difficult to measure through aggregated indicators and would warrant complementary qualitative interpretation.

To attend to these artifacts of (in)consistency, the study employed a cautiously interpretive epistemological shape to interpreting the quantitative findings. The aim was not to derive strong causal or as outcome findings, rather to present indicators within thematic narratives established through document analysis. The purpose of the indicators is interpretive and supportive: to (dis)confirm, or problematize the qualitative narratives developed through legal and policy texts. The quantitative module thus holds a methodological standard, without overstretching its epistemology.

By balancing reliable sources with transparent procedures and an interpretively bounded logic of use, the quantitative element of this research maintains internal logical connectedness and analytical integrity to the multi-modal process. It supports the qualitative rigor of the data from document-based analysis, while ensuring that research outcomes are based on a solid empirical ground of requisite appropriateness for multi-modal, policy-determined doctoral research.

3.5.Comparative Legal Landscape of Public Procurement and Blockchain

3.5.1. Public Procurement Law in Italy: The Shift to Digital, Legal Reform and Anti-Corruption Governance

Public Procurement in Italy is the convergence of domestic legislation (e.g., the Italian Constitution, Legislative Decree n. 50/2016, Government guidelines on public procurement), European Union directives, and judicial administrative decisions or case law. Over the past decade, the journey of this structure has unified into standardizing procedure, transparency, and completely digitalizing all aspects of the contract's life cycle. The culmination of this trajectory is Legislative Decree No. 36 of 31 March 2023 (hereafter, D. Lgs. 36/2023), which repealed the 2016 Code and instituted a binding digital-by-default regime effective 1 January 2024. At the core of this regime are the Piattaforma dei Contratti Pubblici (PCP) and the Banca Dati Nazionale dei Contratti Pubblici (BDNCP), under the stewardship of the National Anti-Corruption Authority (ANAC). The reform intentionally shifts procurement from a document-driven administrative practice to a

data-driven legal process, embedding legal obligations into interoperable technical infrastructures (D. Lgs. 36/2023, arts. 1, 22–23, 25, 28).

Conceptually and architecturally, the Code establishes a unified national ecosystem for digital procurement. Article 22 aims to provide a definition for the ecosistema nazionale di approvvigionamento digitale; Article 23 sets out that the BDNCP is the base data and governance layer; Article 25 governs and regulates one certified digital procurement platform and interoperability; and Article 28 relates to lifecycle transparency and publication obligations. In this context certified e-procurement platforms must connect with the BDNCP and publish legally relevant information using the PCP to assure that procedural actions are performed in a machine-readable, time-stamped, and real-time auditable format (D.Lgs. 36/2023, arts. 22- 25, 28).

Operationally, the digital-by-default regime produces both procedural and infrastructural consequences. Procedurally, all phases—planning, tendering, award, and execution—are to be conducted through certified platforms that support structured, machine-readable data exchanges (including eForms-IT) and are interoperable with the BDNCP. Infrastructurally, only platforms meeting the Code's certification and interoperability conditions may be lawfully employed; this aligns Italy with the EU mandate on electronic means of communication and the metadata harmonization envisaged by the eForms initiative under the public procurement acquis (Directive 2014/24/EU, 2014; D.Lgs. 36/2023, arts. 22–25, 28).

In normative terms, Article 1 states the principio del risultato—aiming for the best quality-price outcome, in full compliance with timeliness--while connecting it to legality, transparency, competition, and proportionality. The principle does not abandon legality or impartiality; it embeds these principles into digital workflows in a way that provides auditability and ex-ante compliance, by means of platform logic and standardized data flows (D.Lgs. 36/2023, art. 1).

Institutionally, ANAC acts both as regulator and system operator. Pursuant to Article 23, ANAC manages the BDNCP and defines required information flows; in coordination with the national rules on certified platforms (Articles 25–26), this establishes a mandatory architecture from 1 January 2024. Complementing the infrastructure, the Code introduces a qualification regime for contracting authorities and central purchasing bodies (Articles 62–63), administered by ANAC, which conditions the exercise of procurement functions on organizational capacity and digital readiness. Where an authority is not qualified, it must rely on a qualified central purchasing body—thereby reducing fragmentation and structurally embedding compliance capacity within the system (D. Lgs. 36/2023, arts. 23, 25–26, 62–63).

Institutionally, the reform recenters the procurement ecosystem around ANAC's governance of the Banca Dati Nazionale dei Contratti Pubblici (BDNCP) and the nationwide publication hub of the Piattaforma dei Contratti Pubblici (PCP). Pursuant to the new Code's digital architecture, Article 22 establishes the ecosistema nazionale di approvvigionamento digitale as a legally unified environment; Article 23 designates the BDNCP as the authoritative repository and control layer for the entire contract life cycle; and Articles 25–26 require that only certified digital platforms—

interoperable with the BDNCP and compliant with the Code's technical rules—may be used by contracting authorities. In this context, Article 28 gives legal force to obligations of transparency and publication. The data sent to the BDNCP through certified platforms is the reference record for transparency, and by publishing through the PCP all data will be readable by machines, traceable, and ex-ante verifiable. As a result, the Code has converted transparency from a mostly ex post documentary exercise into a live legal process driven by data, embedded in the platform's logic (Italy, 2023, arts. 22-26, 28).

To implement Article 28, ANAC adopted a dedicated measure identifying the acts, information, and datasets that must be produced and published across the procurement life cycle, together with timing, formats, and transmission channels. This implementing decision systematizes obligations so that communications, notices, award data, and contract execution updates flow consistently from contracting authorities to the BDNCP and onto the PCP, thereby aligning publication with the Code's dematerialization and interoperability goals. By establishing the unit of disclosure as structured, machine-readable records instead of heterogeneous documents, the measure appears to eliminate the systemic disjuncture between formal publicity and actual public accountability (Autorità Nazionale Anticorruzione [ANAC], 2023a; Italy, 2023, art. 28).

The Code pairs this infrastructural shift with an institutional capacity filter qualification regime for stazioni appaltanti and centrali di committenza is introduced in Articles 62–63. This regime is administered by ANAC and requires that procurement functions be exercised in a way that demonstrates organizational capacity and digital readiness.

Qualification is stratified and function-specific, linking an authority's permitted procurement activities to its certified capabilities (e.g., platform usage, compliance competencies, staffing of key roles). Authorities that don't have the right qualifications must work through a certified central purchasing authority. This rule is intended to reduce fragmentation, increase expertise, and decrease the risk of noncompliance. The regime changes procurement authority from legal entitlement to verifiable competence, within the digital context described in Article 22–25 (Italy, 2023, arts. 22–25, 62–63).

The pre-contenzioso mechanism furthers dispute prevention and legal certainty. Under Article 220 of the code, ANAC is empowered to deliver reasoned opinions—upon the request of the parties to the procurement contract—about legality issues with respect to tender preparation or execution. ANAC's dedicated regulation, adopted immediately after the Code, streamlines the procedure, clarifies admissibility, and sets timelines and evidentiary requirements. Functionally, this mechanism shifts part of the legality assessment to an ex-ante venue, reducing the risk that ambiguities crystallize into post-award litigation and lowering systemic transaction costs. In a digital-by-default setting, pre-contenzioso opinions also dovetail with standardized data flows, since much of the relevant record is already structured within BDNCP-mediated exchanges (ANAC, 2023b; Italy, 2023, art. 220).

The enforcement layer builds upon these precautionary tools. The Code assigns supervisory and sanctioning powers with applicable digital safeguards to ANAC, and the sanctioning regulation of ANAC applies a procedural framework for investigations, contesting a sanction, and imposing a sanction. The regulation utilizes the principle of proportionate response, aligning procedural safeguards with the objectives of the Code and at the same time facilitating proportional intervention against non-compliance (e.g. using a platform that was not assessed as certified, omitting essential transmissions, or breaking the publication responsibilities under Article 28). In other words, oversight is more than retrospective auditing: it is a function of continuous legality, underscored by interoperable systems, standardized metadata, and legal disclosure requirements (ANAC, 2023c; Italy, 2023, arts. 22-28, 222).

The third aspect of the public administration structure hence and functions are limited to make digital compliance not only practical but functional. The Code returns to the idea of the Responsabile Unico del Progetto (RUP) (previously RUP of procedure) as central, now assigning integrated responsibility across phases of public procurement within the digital realm (Italy, 2023, art, 15). At the same time, the wider frame of the public-administration digital layer is one in which every administration is assigned a role, a Rappresentante per la Transizione al Digitale (RTD), with responsibilities of governing the digital processes, including interoperability and security. This has direct requirements that overlap with procurement dematerialization and BDNCP integration. The role of the integrated layer positions RUP and RTD roles associate legal responsibilities to formally named persons, who have the technological authority (the peg) to complete these functions, embedding legality, transparency, and accountability in the operation (Italy, 2005/2023, art. 1(b)). These controls operate within an overarching transparency perimeter that combines national visibility obligations with EU-level transparency expectations. Under the EU procurement acquis, even where contracting authorities have a lawful basis into which to invoke exceptions, they are still also bound by the need to practice electronic communication of the procurement and the publication and ex-post transparency requirements imposed by the relevant legislation (notices, award to name a couple) in order to keep their exceptions from open to view and contestable. The Code aligns Italy with this space by requiring publication through the PCP, embedding rules governing public contracts with metadata that comply with the corresponding EU forms (Italy, 2023, art. 28; Directive 2014/24/EU, 2014). In a similar way, Italy has improved its integrity space by putting whistle-blower protections into place: D.Lgs. 24/2023 transposed Directive (EU) 2019/1937 and expanded protections for disclosers in the public sector and required that administrations establish channels through which to disclose breaches, including in the procurement context. In the digital space, these tools support the data-fuelled supervision because each lowers the information barriers for early detection of irregularities (Directive 2019/1937/EU, 2019; Italy, 2023, D.Lgs. 24/2023).

The reform also moves the point of efficiency to the center of the legality architecture of public procurement. Rather than viewing execution as an afterthought of the administration following an

award, the performance monitoring, variations and payment provisions in Title IV of the Code pulls execution data into the audit trail of the same "stream" as planning (e.g., opening, and decision). Of particular note is the reform's rules on performance, controls (e.g., articles 113-115) that require documentation of delivery timelines and quality compliance contributions to the audit log, modifications must also be logged and recorded in the digital audit trail. The combination of the documentation and audit log allows for ex-ante and ex-post checking of planning vs. quality-performance criteria complied with, and pushes-back against opportunistic behavior like unfounded modifications or extended delays in delivery. Second, though article 108 governing criteria (MEAT) still guides the selections of award (price-quality), the machine-wearable performance documentation will allow for the performance captured at the time of award, against traceable primary sources, and pseudo-universal timestamps and timelines at a future time down-stream. (Italy, 2023, arts. 108, 113-115, 28).

The framework for reputational accountability in Italy operates via prescribed instruments rather than creating new registries. The Casellario informatico—the same repository integrated with the BDNCP under the new Code—remains the reference repository for serious professional misconduct, false declarations, and any other relevant facts for exclusion, so that contracting authorities may test reliability throughout the procedures. By bundling within one registry determinations and sanctions that are interoperable, the Italy framework equalizes jurisdiction in practice by minimizing information asymmetries. The data continuity of award, execution, and matters whereby any grounds for exclusion is very useful for the accurate application of reliability triggers over time (Italy, 2023, art 222; Italy, 2023, arts 94–98).

Lastly, the digital architecture is capabilities-based and technology-neutral but extensible. Although the Code does not prescribe any specific technology—blockchain included—it does prescribe capabilities—traceability, time-stamping, logs integrity, and standardized metadata—that are structurally consistent with distributed-ledger solutions. This is further supported by the earlier statutory recognition of legal definitions for smart contracts and distributed-ledger technologies in Italy (art. 8-ter, as introduced by Law No. 12/2019), which recognizes that smart contracts that meet the guarantees of identity and immutability risks may have the same legal effect as contracts made via traditional means. In other words, section-by-section, all of these instruments offer opportunities for pilot-testing—automated milestone attestations or tamper-evident archival—and keep efficiency, interoperability, data-protected chains, and procedural equivalence within the existing framework of the Code without pre-empting technology choices (Italy, 2019, Law 12/2019, art 8-ter; Italy, 2023, arts 22–25, 28).

The procurement reform cannot be dissociable disentangled from Italy's commitments related to the Recovery and Resilience Facility (RRF). In effect, the PNRR (Piano Nazionale di Ripresa e Resilienza), pertains to mid-level conditions that the Union imposes and national milestones and targets which detail, amongst other things, dematerialization of procurement, the requirement to publish interoperable (with the BDNCP) data and necessary and systematic monitoring of contract life cycles. In terms of the legal-operational connection, Decree-Law No. 36/2022, converted by

Law No. 79/2022, imposes acceleration and various compliance obligations on public entities that manage RRF resources, all to make procurement data available electronically/in real-time/or as close to real-time as possible to nationally coordinated monitoring infrastructures. These measures link fiscal conditionality to administrative legality, therefore meaning publication on certified platforms, using standardized metadata (e.g., eForms-IT) and publishing via the PCP/BDNCP being recorded is, no longer merely an administrative best practice; it is a condition of further and continued access to publicly funded EU resources (Italy, 2021; Italy, 2022; Regulation (EU) 2021/241).

The ReGiS platform—a comprehensive digital infrastructure initially developed under the Ministry of Economy and Finance as the defining registry—and the fulcrum of this fiscal-legality bridge—will presumably operate as the repository for PNRR interventions. ReGiS is designed to interoperate with sectoral systems—and most significantly the BDNCP—which ultimately predicts that procedural legality, financial reporting, and execution of contracts should all be triangulated on a like-for-like data architecture. Ultimately, the whole cycle of procurement that is done under Articles 22–25 and 28 of the Code necessarily project their legal metadata and potentially coterminous/explanatory records across the broader PNRR monitoring context, allowing aggregate checks of eligibility, compliance with publication duties, and observance of the terms and conditions of award and execution to be made. When reconciled, these processes generate strong ex-ante and ex-post checks without requiring and therefore duplicating taxpaying administrative burdens, because the same certified data utilities used for the purposes of procurement transparency (Italy, 2023; Ministry of Economy and Finance, 2022).

The multiple-layered accountability environment operates trans-nationally. By interlinking the traceability obligated by the Code and PNRR reporting, Italy allows trans-national cross auditing by Italian and European inspectors. At the national level, the Corte dei conti uses standardized, time-stamped procurement data when checking for legality and accounting; at the European level, OLAF and EPPO can obtain structured data and documentation from the public bodies under their jurisdiction for any and all proceedings, provided that there is a reasonable basis to suspect fraud, corruption, or maladministration of EU funds. The ability to export legitimate, machine-readable histories of procedures—planning, notices, decisions of award, modifications, and payments—creates evidential frictionless mechanisms that limit the distance between anomaly detection and remedial action (Italy, 2023; Regulation (EU, Euratom) No 883/2013; Council Regulation (EU) 2017/1939).

In this schema, the PCP is a single point of intersection that acts as the legal-open gateway for public disclosure of procurement activities, while the BDNCP is the canonical backend for integrity, oversight and cross-system exchange. In compliance with the Code's Article 23, public administration must publish all procurement related records through the PCP and all procurement agents must submit their procedural records to the PCP exclusively. This close linkage removes fragmentation from local portals and ensures that publication assumes some dimension of legally binding effect as it is based on records established by the validated framework of the BDNCP.

Publication is not merely declarative; it is a legal form of data-driven transparency: notice records, decisions and updates to execution record may be made a part of the publicly, and, where agents are concerned, verifiably compliant audit-trail (Italy, 2023, arts. 23, 28).

The ability to induce meaningful consequences for violations—based on the Code's binding publication/transmission duties (Article 28) linked to ANAC's oversight powers (Article 222) and sanction regulation—complements the remedial elements and disassociates compliance from pure remediation. When a public administration uses an un-certified platform, fails to undertake a mandatory transmission process, or does not comply with duties of publication by virtue of the adoption of invalid timing or content, ANAC may take steps proportionate to the nature of the particular failure and the systemic risk associated to the non-compliance. As such, transparency and digital traceability shift from being aspirational concepts of policy to being enforceable rights and obligations. While the layers of compliance have moved the regime from a paper process of compliance to a legally enforce process in a platform space active at the point of use—undetected violations can also be discovered by the targets of the regime through data validation processes, which ceteris paribus indicate, in the administrative legislation, the record the administration will create (ANAC, 2023c; Italy, 2023, arts. 22–28, 222).

In conclusion, the PNRR-resourced reforms are establishing a constitutional logic within the digital procurement ecosystem. The Code seeks to achieve fields of transparency, impartiality, and good administration through interoperable systems which employs standardized formats and different, widely held terms of data model which impart established constitutional principles are practical - for the framed codes in an accountability regime to work, they need to allow for and ultimately respect technology neutrality. However, the framework does not inscribe any particular technology into the context of integrity; rather, it outlines and provides codification to, basic legal characterizations of the process, and (i.e. including but not limiting to) time-stamped traces of the process and integrity of logs of standard formats. This presents an open migration space for future pilots using new and emerging technology on two bases; that they respect interoperability and data protection work, and that they maintain a level equivalence in the process (Italy, 2019; Italy, 2023, arts. 1, 22–25, 28).

Integrity protection in the reformed framework applies at both the individual and organizational levels. On the individual level, conflicts of interest protections are included in Article 16 of D.Lgs. 36/2023, which defines the situations in which any subject acting in the award or execution—be it public official or outside expert—has a direct or indirect interest that is likely to compromise the impartiality and independence. The provision requires ex ante declarations, abstention duties, and traceable documentation of checks, thereby linking ethical compliance to the same machine-readable record that governs procedural steps. Because these safeguards are embedded in the certified platform workflow, conflicts and recusals—together with the identity of responsible officials—become part of the authoritative data trail and are thus auditable across the life cycle (Italy, 2023, art. 16; arts. 22–23, 28).

At the organizational level, the Code couples' legal obligations with role design and professionalization. Article 15 confirms the centrality of the Responsabile Unico del Progetto (RUP), who coordinates phases and ensures completion of the intervention in line with legal and technical requirements across planning, tendering, award, and execution. The Code's qualification regime (arts. 62–63) then ties the exercise of procurement functions to demonstrable digital readiness and organizational capacity, effectively making competence—not mere entitlement—the gateway to tender management .Simultaneously, the broader public-sector digital framework consists of a requirement for every authority to appoint a Responsabile per la Transizione al Digitale (RTD) under Article 17 of the Codice dell'Amministrazione Digitale (CAD), with responsibilities relating to interoperability, security, and governance of digital processes. The RUP–RTD coupling links legal accountability to technical authority, ensuring that procurement duties are executable within the dematerialized ecosystem the Code prescribes (Italy, 2005/2023, art. 17; Italy, 2023, arts. 15, 22–28, 62–63).

These structural arrangements are complemented by the preventive dispute-resolution tool of pre-contenzioso. Under Article 220, ANAC may issue reasoned opinions—on party request—during tender preparation or execution, supplying authoritative guidance before controversies crystallize into litigation. ANAC's implementing regulation streamlines admissibility, timelines, and evidentiary submissions and aligns the procedure with the Code's data architecture, so that the digital dossier transmitted via certified platforms provides the factual baseline for legal assessment. This mechanism minimizes transaction costs, facilitates the harmonization of administrative practices, and promotes legal certainty in an environment in which compliance is increasingly data-verified, instead of asserted on a piece of paper (ANAC, 2023b; Italy, 2023, art. 220).

The enforcement aspect closes the loop between obligation and accountability. ANAC's supervisory and sanctioning powers under Article 222 are specified to the digital regime and actualized through ANAC's regulation on sanctions. Where authorities do not utilize a certified platform, do not transmit information to the BDNCP as mandated, or do not fulfill their publication requirements under Article 28, the Authority may launch proceedings, calibrated to the seriousness and systemic elements of the infraction. Since all of these obligations take the form of standardized, time-stamped flows - that allow deviations to be identified, in advance of implementation, through normal validations and audit trails - enforcement is moved away from an ex-post check of documents and to ongoing assurance of legality by ANAC (ANAC, 2023c; Italy, 2023, arts. 22-28, 222).

Execution-phase controls further entrench accountability. The Code integrates award, execution, modification, and payment into one auditable chain. Articles 113–115 require that execution conditions and any variations be documented in the digital record, enabling monitoring against the award's substantive commitments and legal limits. Instead of inventing new reputational databases, the system relies on established instruments—most notably the Casellario informatico

(now coherently integrated with the BDNCP under the new Code)—to consolidate exclusion-relevant facts (e.g., grave professional misconduct, false declarations) across procedures. In this way, the framework reduces information asymmetries and strengthens equal treatment by ensuring that reliability assessments are portable from one procedure to the next (Italy, 2023, arts. 113–115, 94–98, 222).

Finally, the integrity perimeter is reinforced by Italy's general anticorruption and transparency legislation. Law No. 190/2012 mandates the institutionalization of the Responsabile della prevenzione della corruzione e della trasparenza (RPCT) and the adoption of triennial anticorruption plans within each administration, while D.Lgs. 33/2013 systematizes publication obligations and civic access. Read alongside Article 28 of the procurement Code, these instruments ensure that the publicity of acts and the auditability of data converge within a single compliance pipeline: publication via the PCP (anchored in BDNCP-validated flows) is not just informative but juridically constitutive of transparency in procurement, and RPCT oversight provides the organizational guarantee that these flows are sustained and continuously improved over time (Italy, 2012; Italy, 2013; Italy, 2023, art. 28).

Taken together, the reforms recast Italian public procurement as a digitally structured, legally integrated, and audit-ready system. With PCP as the exclusive gateway for legally effective publication and BDNCP as the canonical back-end for integrity and supervision, the Code's architecture binds procedural legality to certified, interoperable data flows. Transparency and traceability are no longer ancillary ideals but justiciable obligations embedded in Articles 22–25 and 28, while oversight and sanctioning powers—coherently framed in Article 222 and ANAC's implementing regulation—translate compliance from episodic paper checks into continuous, data-driven legality assurance. This transformation implements the EU acquis on electronic procurement and the principle of effectiveness in remedies by ensuring that each procedural step generates a machine-readable, time-stamped trail capable of sustaining ex-ante validation and ex-post review (Directive 2014/24/EU, 2014; Italy, 2023).

Yet the model remains attentive to institutional capacity and due process. The qualification regime (Arts. 62–63) conditions the exercise of procurement functions on verifiable organizational and digital readiness, channeling activity to competent entities and thereby reducing fragmentation and exposure to risk. Role design reinforces this orientation: the RUP (Art. 15) anchors legal accountability across phases, while the RTD under the CAD (Art. 17) supplies the administrative authority and technical governance required for dematerialization and interoperability. Integrity safeguards—including conflict-of-interest controls (Art. 16), structured transparency (Art. 28), and the Casellario informatico integrated with the BDNCP (Art. 222)—ensure that reliability assessments and exclusion grounds are portable and consistently applied throughout the market, enhancing equal treatment and trust (Italy, 2005/2023; Italy, 2023).

Doctrinally, the framework is technology-neutral yet extensible. The Code does not prescribe any single technology for integrity assurance; rather, it specifies legal properties—traceability, time-

stamping, integrity of logs, standardized formats, and interoperability—that any conforming solution must realize. This legal-technological posture is compatible with distributed-ledger approaches and smart contracting, whose legal effects have been expressly recognized in Italian law since Law No. 12/2019, Art. 8-ter (identity assurance and immutability as predicates for equivalence). Accordingly, pilots involving automated milestone attestations, tamper-evident archival, or machine-verifiable performance data can be assessed within the Code's existing principles—without derogating from competition, transparency, or due process—provided they respect interoperability and data-protection constraints (Italy, 2019; Italy, 2023).

At the EU–national interface, the link to the Recovery and Resilience Facility (RRF) cements fiscal conditionality to administrative legality. Through the PNRR and the ReGiS platform, procurement data generated under Articles 22–25 and 28 are triangulated with financial reporting and execution records, enabling consolidated, multilevel oversight (national audit and EU antifraud/prosecutorial control) while avoiding duplicative burdens. In this respect, the Italian approach operationalizes constitutional principles—transparency, impartiality, good administration—via interoperable systems and standardized data, making legality verifiable by design and reinforcing accountability across jurisdictions (Italy, 2021; Regulation (EU) 2021/241).

To summarize, the D.Lgs. 36/2023 and its implementing acts, do not only digitize old processes, they instead redesign the legal method of public contracting. The regime incorporates compliance into a basis of procurement, by integrating mandatory platform certification, unified data governance, structured transparency, proactive dispute avoidance, and strategically graduated enforcement. This legal-technical synthesis is not only compatible with future blockchain integration; it readies the system for it—so long as forthcoming technical standards and administrative guidance translate the Code's legal properties into interoperable, secure, and rights-preserving implementations. In domains where immutability, automation, and verifiability are indispensable to safeguarding the public interest, the Italian model provides a defensible, constitutionally grounded pathway for aligning public law integrity with technological modernization (Italy, 2019; Italy, 2023; Directive 2014/24/EU, 2014).

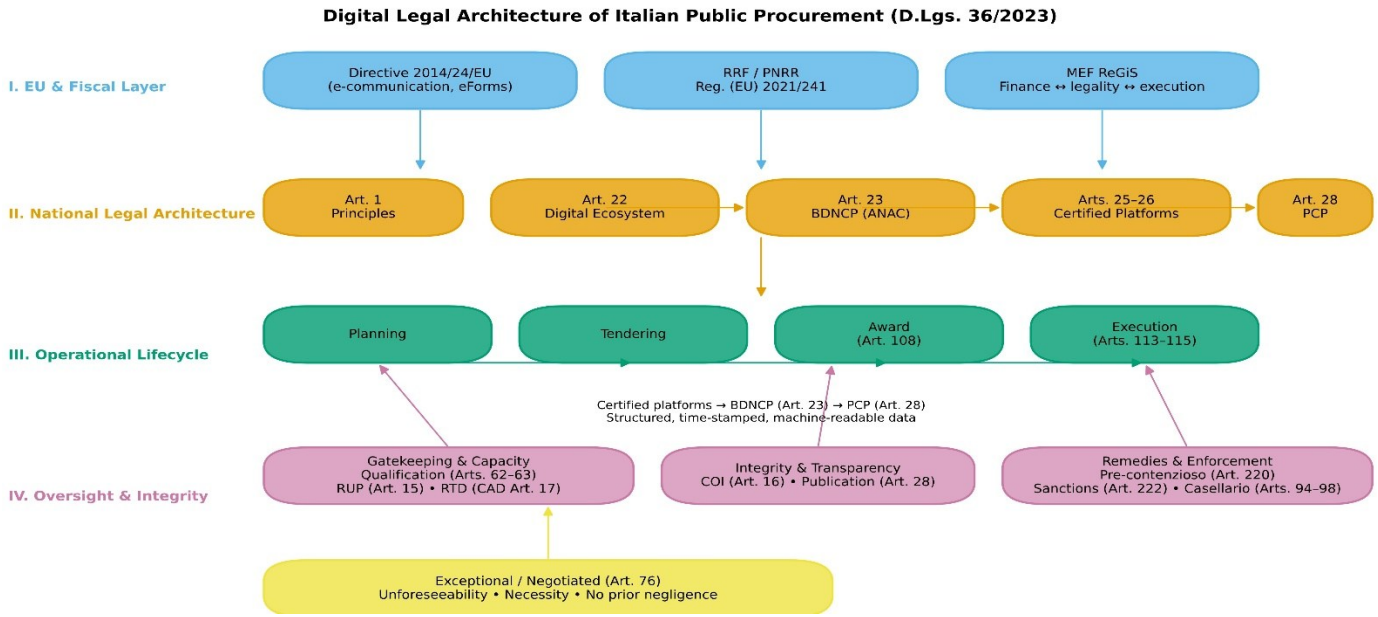

Figure 2. Digital legal architecture of Italian public procurement (D.Lgs. 36/2023).

Note. Pipeline: certified platforms (Arts. 25–26) to BDNCP (ANAC, Art. 23) to PCP; transparency under Art. 28. Lifecycle: planning, award (Art. 108), execution (Arts. 113–115) within the core (Art. 1; Arts. 22–23, 25–26, 28). Oversight/integrity: qualification (Arts. 62–63), RUP (Art. 15), COI (Art. 16), pre-contenzioso (Art. 220), sanctions/Casellario (Art. 222; Arts. 94–98). External constraints: Directive 2014/24/EU, Reg. (EU) 2021/241 (ReGiS). RTD under CAD Art. 17.

Italy's 2023 Public Contracts Code reconceives procurement as a digitally enforced legal process in which compliance is evidenced by certified data flows, not ex-post documentation. The national "ecosistema di approvvigionamento digitale" (Art. 22) articulates the technical–legal boundary, while ANAC's Banca Dati Nazionale dei Contratti Pubblici (BDNCP) will act as the controlling authoritative stratum (Art. 23) and offers legally compliant coded construction in data flows that contracting authorities will use (Arts. 25–26). Transparency has now shifted from elective publication practice into an enforceable obligation shaped by machine-readable disclosure through the Piattaforma dei Contratti Pubblici (PCP), which is automatically sourced from BDNCP-validated records (Art. 28; ANAC, 2023a). This alignment embeds legality ex ante: every procedurally deliberate act (notice, clarification, award decision, modifications) must traverse machine readable, time-stamped channels structured as an auditable and transparent pathway that is both fit for preventive monitoring and judicial scrutiny (Italy, 2023, Arts. 22–23, 25–26, 28).

This architecture takes the lifecycle as a single dematerialized chain. Award remains fixed on EU qualité–prix criteria (Art. 108 MEAT), whereas executing the contract is governed by Title IV, which provides for documentation of performance, variations, and payment (e.g., Arts. 113–115).

As intended acts will initiate on compliant platforms and be recorded to the BDNCP before published on the PCP, the substantive promises verified at the award stage can be audited at the downstream execution stage against structured performance evidence (Italy, 2023, Arts. 108, 113–115, 28). The qualification regime for stazioni appaltanti and centrali di committenze (Arts. 62-63) polices capacity, tying procurement functions to demonstrable organizational and digital competency. Procurement functions without qualification operate through qualified central bodies (Italy, 2023) (Arts. 62-63). The design of roles connects the RUP, responsible for integrated accountability of the project through all phases (Art. 15), with the public administration's RTD structure under the Codice dell'Amministrazione Digitale (Art. 17), reflecting the mapping of legal obligations to technical authority in terms of interoperability and security (Italy, 2005/2023) (Art 17; Italy, 2023) (Art 15). Integrity protections require and require conflict-of-interest prevention and declarations (Art. 16), to centralize reliability assurances in the Casellario informatico (Arts. 94-98, 222). Dispute prevention and enforcement mechanisms are tuned to the digital realm: pre-contentious opinions offer ex ante legality opinion based on the BDNCP file (Art 220; ANAC, 2023b) and ANAC's sanction powers (Art. 222) are coupled with the sanctioning regulation (ANAC, 2023c). Exceptional or negotiated procedures are exceptions as a matter of law, under strict circumstances—foreseeability, necessity and lack of prior fault—and justification is required (but structured) to be written in the same task (Art. 76).

Finally, the architecture is technology-neutral and extensible. The Code prescribes legal properties for compatibility with distributed ledger solutions—traceability, time stamping, integrity of logs, interoperability—and smart contracts where guarantees of identity and immutability are met (Law 12/2019, Art. 8-ter), are already legally acknowledged by national law. In respect of the EU-national interface, required e-communication and standardized notices under Directive 2014/24/EU, plus fiscal conditionality of the Recovery and Resilience Facility, are operationalized in Italy through the PNRR monitoring environment (Reg. (EU) 2021/241) which allows procurement data created under Arts. 22-28 to be used to match multi-level oversight mechanisms, without duplicative reporting. In summary, D. Lgs. 36/2023 does not digitize procedure; its re-engineers' legality as data, making transparency and legality affirmatively within and accountable parts of procurement process (Directive 2014/24/EU, 2014; Regulation (EU) 2021/241; Italy, 2019; Italy, 2023).

Italy's D.Lgs. 36/2023 establishes a digitally codified procurement ecosystem, incorporating certified platforms, standardized eForms-IT, and BDNCP anchoring, which collectively convert procedures into auditable data flows under ANAC supervision. Ledger artefacts can enhance this framework by integrating with certified workflows, maintaining human authorization, and fulfilling GDPR-related obligations such as accuracy, minimization, and provisions for erasure. The optimal approach involves selective anchoring (hash/timestamp) alongside the preservation of canonical records in certified repositories, which are cross-referenced for review purposes. D.Lgs. 36/2023, articles 1, 22–25, 28; ANAC.

3.5.2. Public Procurement Law in Canada

Canada's federal procurement regime is founded on a clear statutory core complemented by binding administrative instruments and layered oversight. The Financial Administration Act delegates financial and contracting authorities within a framework of ministerial responsibility and internal control, while the Government Contracts Regulations establish a default duty to compete and specify limited, exhaustively framed exceptions to competition such as sole-source availability, national security, or extreme urgency (Financial Administration Act, R.S.C., 1985, c. F-11; Government Contracts Regulations, SOR/87-401). Operationally, this legislative architecture is given contemporary effect by the Directive on the Management of Procurement, which defines procurement as an end-to-end life-cycle activity from need identification through contract close-out; embeds the principles of fairness, openness, transparency, and value for money; and integrates trade-agreement disciplines, risk management, and recordkeeping requirements into departmental systems of internal control (Treasury Board of Canada Secretariat [TBS], 2023). The interaction of statute and directive is not merely formal: it is the means by which governments translate constitutional accountability for public expenditure into auditable procedures, standardized documentation, and reviewable decision-making.

Institutionally, the federal system demonstrates a hybrid model that incorporates a common service provider and delegated departmental authorities. The common service provider does the heavy lifting for federal buying, especially for common-good procurements, complex service contracts, and unique acquisitions, while departments and agencies conduct acquisitions directly, within their assigned procurement authorities, as long as they follow statutory requirements and TBS Policy suite (TBS, 2023). Oversight and remediation are layered, promoting legality and respect for process. The Office of the Procurement Ombudsman provides independent review of complaint files, practice review reports, and dispute resolution services for procurements that are below the Ombudsman's monetary thresholds; for designated, covered procurements, above domestic and international trade-agreement thresholds, bid challenges are received and heard by the Canadian International Trade Tribunal, a quasi-judicial tribunal, that can make recommendations for corrective action and/or compensation, with scope for judicial review on previously established principles of administrative law (Office of the Procurement Ombudsman [OPO], 2024; Canadian International Trade Tribunal [CITT], 2023). Ex post scrutiny by the Office of the Auditor General—and through performance audits on a regular basis—adds a level of control for the system that can invoke remedial actions and/or although generally not amend Treasury Board guidance where systemic flaws are found (Office of the Auditor General of Canada [OAG], 2021). In this regard, where legal adherence exists in structured and repetitive administrative practice due process is mirrored by legal accountability.

Digital modernization has integrated federal e-sourcing, publication of notices and, bid submission on one platform that standardizes notice content, templates, structured data capture, and file organization. In doctrinal terms, this infrastructure is relevant because it renders legality: the standardized fields and validation routines allow confirmation of the recognizing application of

competition rules, a record of evaluation that is traceable, and a record that is more auditable without dissipating the requirement for human judgement on legal issues. At the same time, supplier onboarding is essentially structured in two parts: ie. e-bidding is not the same as able to be successful (receiving an award and the possibility of receiving payment) participating bidders must register in the federal supplier system to ensure eligibility with respect to identity verification and tax compliance (Public Services and Procurement Canada [PSPC], 2024a). This separation between functions has implications from a legal accountability perspective. In practice this divides procurement 'workflow' on the e-sourcing platform and the registry for an award. It is a significant function of two-part structure' as it helps define the moment in time when verification of a bidder's legal ability to contract from a tax perspective occurs when contracts/ agreements' are formed through a procurement process.

Integrity, security, and privacy protections are embedded across the procurement life cycle. The federal Integrity Regime, implemented through the Ineligibility and Suspension Policy, enumerates offences, disclosure obligations, and mitigating conditions that can render supplier's ineligible or conditionally eligible to contract; mandatory certification clauses in solicitation and award documents provide the legal mechanism for system-wide application (PSPC, 2024b). Through the Contract Security Program and the Security Requirements Checklist, security requirements are scaled to the sensitivity of the work, so that organizational and personnel screening are aligned with classifications of information and assets while maintaining proportionality (PSPC, 2024c). When personal information is collected or processed through procurement files, such as in integrity declarations or security screenings, the Privacy Act and the federal privacy regulator's guidance establish necessity, proportionality, and data minimization in such a way as to preserve the due-process and confidentiality interests without unnecessarily obstructing transparency and competitiveness (Office of the Privacy Commissioner of Canada [OPC], 2022). All of these protections, collectively, give specified effect to the constitutional and administrative-law expectation that public contracting be efficient and rights-respecting.

Finally, Canadian procurement practice is shaped by common-law tendering doctrine and by binding trade obligations. The Supreme Court's jurisprudence—most notably Martel Building, Double N Earthmovers, and Tercon Contractors—has clarified the Contract A/Contract B framework, the content of the duty of fairness and equal treatment in evaluation, and the modern test for enforcement of exclusion clauses (Martel Building Ltd. v. Canada, 2000; Double N Earthmovers Ltd. v. Edmonton [City], 2007; Tercon Contractors Ltd. v. British Columbia, 2010). These principles operate alongside the procurement disciplines found in the Canadian Free Trade Agreement, the Comprehensive Economic and Trade Agreement, and the WTO Agreement on Government Procurement, which entrench non-discrimination, transparency, advance publication, and domestic review mechanisms across federal and sub-federal entities (Canadian Free Trade Agreement Secretariat [CFTA Secretariat], 2017; Global Affairs Canada [GAC], 2023; World Trade Organization [WTO], 2014). The combined effect is a multi-layered legal environment in which statutory authority, administrative policy, judicial doctrine, and international commitments

mutually reinforce procurement decisions that are both contestable and auditable—conditions essential to integrity and to future-ready digital modernization.

At sub-federal level, procurement authority derives from provincial and territorial jurisdiction over property and civil rights and over the organization of public administration, producing distinct but convergent regimes across Canada. In practice, statutory and directive-based frameworks at the provincial and territorial levels are harmonized through internal and international trade disciplines—most notably Chapter Five of the Canadian Free Trade Agreement, together with Canada's sub-central commitments under the revised WTO Agreement on Government Procurement and relevant bilateral agreements—which require non-discrimination, transparent notice, and domestic review mechanisms for covered procurements (Canadian Free Trade Agreement Secretariat, 2017; World Trade Organization, 2014; Global Affairs Canada, 2023). This multilevel architecture preserves provincial autonomy in institutional design while aligning core procedural guarantees with federally accepted trade standards.

Concrete provincial models illustrate this alignment. Québec's Act Respecting Contracting by Public Bodies codifies foundational duties of transparency, competition, and accountability for ministries, agencies, health and education networks, and state enterprises, and it anchors independent oversight through the Autorité des marchés publics, which may receive complaints, audit processes, and order corrective measures to restore fairness (Act Respecting Contracting by Public Bodies, CQLR c C-65.1; Autorité des marchés publics, 2023). The Broader Public Sector Procurement Directive establishes mandatory process controls, requirements and consideration for designated public entities in Ontario, including: competitive procurement that exceeds threshold amounts, risk of conflict-of-interest, documentation integrity, and obligation for debriefings that institutionalizes fairness and equal treatment in the procurement process that is beyond the scope of common-law tendering doctrine (Management Board of Cabinet, 2011). Other provinces adopt analogous instruments—whether statutory or policy based—that internalize competition rules and embed auditability requirements in procurement files, with municipal authorities typically operating under enabling statutes and procurement by-laws that reflect the same design principles through standardized templates, delegated authority matrices, and vendor-performance procedures. Although institutional vocabulary and oversight models vary, the functional commitments to transparency, competition, and contestability remain consistent across jurisdictions because they are sustained by trade-agreement disciplines and by the administrative-law obligation to act fairly.

The doctrine of administrative law provides the doctrinal connection between policy and justiciability. Courts in Canada ultimately review procurement decisions through the lens of legality, procedural fairness, and reasonableness --- as applied in the modern framework for judicial review of administrative action - recently enunciated by the Supreme Court. Accordingly, the post-Vavilov reasonableness examination of the procurement authority's decision will be concerned with justification, intelligibility, and responsiveness to the statutory and policy context, with courts accorded deference to clear evidentiary indicia of statutory constraint, or the

establishment of a recognized special oversight or adjudicative framework (Canada [Minister of Citizenship and Immigration] v. Vavilov, 2019). The view of administrative law applied in the context of competitive tendering in non-trade dispute and trade law, creates layered frameworks under the tendering process. The private law framework for procurement - Contract A/Contract B model - and the private remedies available under the bid challenge provisions in trade agreements creates two regulatory frameworks in parallel that reflects procedural regularity and substantive discretion (Canada [Minister of Citizenship and Immigration] v. Vavilov, 2019). Practically, this means that a procuring authority has ongoing obligations to demonstrate audit trails that show the criteria for evaluation are consistent, that they applied those criteria consistently, and that there was a reasoned basis for any departures from the competition, or the applicable standard. The procuring authority must be able to demonstrate reasonable decisions that can be defended should it be reviewed.

Access to information and privacy laws at the provincial and territorial levels further condition procurement governance by establishing disclosure baselines for records and privacy safeguards for personal data collected in the course of supplier vetting, integrity declarations, and security screening. Statutes such as Ontario's Freedom of Information and Protection of Privacy Act, Québec's Act respecting Access to documents held by public bodies and the Protection of personal information, and British Columbia's Freedom of Information and Protection of Privacy Act require institutions to balance transparency with legitimate exemptions for third-party commercial information, security, and personal privacy, and they impose duties of accuracy, necessity, and proportionality in the handling of personal information (Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31; Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR c A-2.1; Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165). Because procurement files increasingly comprise structured digital data and metadata, these statutes reinforce the need for disciplined record design: evaluation documentation must be sufficiently granular to support meaningful debriefings and defensible decisions, yet curated to avoid over-collection or improper disclosure of sensitive data. Importantly, the coexistence of access and privacy regimes with trade-agreement review rights ensures that suppliers have both informational and remedial pathways to contest unfair treatment, a feature that enhances market confidence and deters opportunistic process deviations.

Taken together, these provincial-territorial arrangements demonstrate a coherent legal ecology: statutes and directives codify process duties; administrative law polices justification and fairness; access and privacy laws structure information flows and data protection; and trade-agreement disciplines align sub-federal practice with national and international transparency norms. This coherence is not accidental—it reflects sustained legal adaptation to the realities of digital procurement and multi-jurisdictional market participation. It also provides the doctrinal foundations required to assess the legal feasibility of distributed ledger technologies and smart-contract mechanisms in public procurement, an assessment that turns on how these innovations interact with competition rules, record-keeping and disclosure duties, privacy safeguards, and

reviewability standards developed across both federal and provincial systems. The next pages use this foundation to analyze the specific legal provisions that bear on electronic contracting, evidentiary admissibility, automation, and code-as-text duality in the Canadian context.

The legal conditions for distributed ledger technologies and smart-contract mechanisms in Canadian public procurement are best understood through Canada's technology-neutral framework for electronic transactions, evidence, and privacy. At the federal level, the Personal Information Protection and Electronic Documents Act recognizes electronic documents and secure electronic signatures within a set of statute-specific amendments, while the Canada Evidence Act establishes criteria for the admissibility and weight of electronic records, focusing on system integrity, reliability of the recording process, and the accuracy of the resulting data rather than on any particular technology (Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5; Canada Evidence Act, R.S.C. 1985, c. C-5). Across the provinces and territories, the Uniform Law Conference of Canada's Uniform Electronic Commerce Act has been widely implemented and confirms that a legal requirement for a "writing" or "signature" can, in most contexts, be satisfied electronically and that contracts concluded by electronic agents are valid, subject to ordinary rules of formation, capacity, and legality (Uniform Law Conference of Canada, 1999; see also Electronic Commerce Act, 2000, S.O. 2000, c. 17). In doctrinal terms, these instruments suggest that procurement processes may incorporate cryptographic signatures, time-stamping, and automated confirmations without displacing existing principles of offer and acceptance, consideration, and intention to create legal relations; the enforceability of the contract in smart-contract systems remains as long as it shows assent and maps to the parties' allocative and remedial intentions. (Zweig & Carroll, 2022).

Evidentiary rules are similarly hospitable to ledger-based records provided that provenance and integrity can be demonstrated. Under the Canada Evidence Act's electronic-documents regime, courts assess reliability by reference to the methods by which data were recorded, stored, and maintained, the security of the system, and the presence of controls against alteration. A distributed ledger can satisfy these criteria where there is credible proof of hashing, consensus, and immutability across nodes; yet the ledger's technical properties do not automatically dispense with foundational requirements such as authenticity, continuity of custody, and the ability to explain anomalies or forks. In the procurement setting, this implies that any blockchain-anchored record—such as the timestamping of bid submissions or contract modifications—should be paired with a conventional records-management schema, including metadata standards, role-based access controls, and audit trails intelligible to non-technical reviewers, so that the record is both legally admissible and operationally reviewable (Canada Evidence Act, R.S.C. 1985, c. C-5).

Procurement, as a public decision-making process, is governed by privacy and administrative law constraints that limit the design possibilities for distributed ledger technology (DLT). The collection or processing of personal information, including beneficial-ownership attestations, declarations of integrity, or key-holder credentials, is regulated by the Privacy Act. Federal institutions are required to adhere to principles of necessity, proportionality, and data minimization

in their actions. Private-sector suppliers are subject to the fair-information principles outlined in the Personal Information Protection and Electronic Documents Act, as well as comparable provincial regulations (Office of the Privacy Commissioner of Canada, 2022; Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5). Immutable ledgers present distinct challenges to the principles of data minimization and retention limitation, as well as to access and correction rights. Due to challenges related to data minimization, retention limitations, and access rights, legally defensible designs necessitate selective anchoring, such as the preservation of documents off-chain in controlled repositories, meticulously planned retention schedules aligned with relevant archival legislation, and well-defined protocols for key rotation and revocation. From an administrative law perspective, the implementation of an automated process to achieve specific procedural steps does not negate the obligation of fairness. Automated sequencing must remain auditable, provide transparent reasoning, and allow for exceptions in unusual cases, ensuring that outcomes are not arbitrary. Canada's Directive on Procurement Management and Directive on Automated Decision-Making -Both elements support this stance regarding the procurer as a public entity by mandating appropriate documentation for all actions, some degree of human oversight, and a risk assessment when automated tools affect rights or eligibility (Treasury Board of Canada Secretariat, 2023; Treasury Board of Canada Secretariat, 2020).

Common-law principles add further contours to DLT adoption in procurement. The tendering jurisprudence that structures Contract A (the bidding process) and Contract B (the performance contract) demands clarity in the terms that govern compliance, evaluation, and privilege or exclusion clauses. Encoding portions of these terms as executable logic can enhance consistency and reduce discretionary opacity; however, enforceability ultimately turns on the text against which compliance is judged and on whether bidders were given a fair opportunity to understand and meet those requirements. The Supreme Court’s approach to exclusion clauses and fairness—most prominently in Martel Building, Double N Earthmovers, and Tercon Contractors—suggests that hybrid specifications (natural-language terms paired with formalized schemas or code) are preferable to “code-only” obligations because they preserve intelligibility for suppliers, reviewers, and courts while enabling automated checks at scale (Martel Building Ltd. v. Canada, 2000; Double N Earthmovers Ltd. v. Edmonton [City], 2007; Tercon Contractors Ltd. v. British Columbia, 2010). Where conflicts arise between code execution and contractual text, adjudicators will look to the parties’ manifested intentions, the allocation of risk evident in the solicitation and award documents, and the reasonableness of the procuring entity’s interpretation under public-law standards of justification.

Finally, federalism and jurisdictional diversity condition implementation pathways. Contract law, property and civil rights, and evidence rules are primarily provincial matters, whereas federal departments remain bound by federal statutes, Treasury Board instruments, and international procurement obligations. As a result, cross-jurisdictional solutions—such as ledgers used by both federal and provincial bodies or by municipal authorities participating in federally funded programs—must accommodate heterogeneous electronic-commerce and evidence statutes, varied

privacy obligations, and different oversight forums. The prudent legal posture is therefore incremental: adopt DLT modules that are compatible with the strictest applicable regime in a given procurement workflow (for example, off-chain storage with on-chain hashes plus dual-format specifications), document the risk analysis and exception handling ex ante, and ensure that bid-challenge and audit bodies can examine both the technical artefacts and their natural-language counterparts. In this way, blockchain can enhance auditability and traceability without compromising the doctrinal pillars of Canadian procurement law.

Assessing the legal feasibility of distributed ledger technologies and smart contracts in Canadian public procurement requires translating doctrine and policy into implementable governance and design choices. The governing premise is technological neutrality: Canadian contract, evidence, and administrative law do not privilege any particular architecture but insist that processes remain fair, intelligible, and reviewable. Under tendering doctrine, compliance conditions and evaluation rules form part of Contract A; they must be communicated clearly, applied consistently, and framed so that bidders can understand what is required to remain compliant (Martel Building Ltd. v. Canada, 2000; Double N Earthmovers Ltd. v. Edmonton [City], 2007). If any component of compliance checking is executed in code—such as deadline validation, mandatory form checks, or arithmetic scoring—its logic must be anchored in the solicitation text and supported by an auditable record of how the rule was triggered in each file. Where exclusionary consequences follow automatically from coded checks, the modern approach to exclusion clauses obliges a reasoned reconciliation between the text and the automation, with space for narrowly tailored discretion to avert disproportionate results in unusual cases (Tercon Contractors Ltd. v. British Columbia, 2010). In administrative-law terms, the justification requirement after Vavilov means procurement authorities should be able to demonstrate, on the record, how automated steps fit within the statutory and policy framework and how exception handling preserved fairness when atypical facts arose (Canada [Minister of Citizenship and Immigration] v. Vavilov, 2019; Treasury Board of Canada Secretariat [TBS], 2023).

A second pillar concerns evidentiary robustness. The Canada Evidence Act assesses electronic records by reference to system integrity, controls against alteration, and reliability of the recording process. A permissioned ledger with well-documented consensus, hashing, and key management can satisfy these factors, but it does not obviate the need for provenance, chain-of-custody documentation, and explanations for anomalies or forks (Canada Evidence Act, R.S.C. 1985, c. C-5). To secure admissibility while maintaining operational practicality, legally resilient designs favour selective anchoring: the authoritative documents, evaluation worksheets, and communications remain in a managed repository governed by records schedules, while ledger entries store cryptographic digests and time-stamps that make tampering evident. This dual structure yields two complementary artefacts for review bodies—a human-readable file that supports debriefing and reason-giving, and a tamper-evidence layer that speaks to integrity. Importantly, this approach aligns with the Uniform Electronic Commerce Act's principle that electronic records meet "writing" and "signature" requirements when reliable methods are used to

identify the signatory and indicate approval, without mandating a particular technology (Uniform Law Conference of Canada, 1999; Electronic Commerce Act, 2000, S.O. 2000, c. 17).

Privacy and data-protection constraints delineate a third design boundary. Procurement files may contain personal information about vendor representatives, subcontractors, or beneficial owners. Federal institutions must satisfy necessity, proportionality, accuracy, and retention-limitation requirements under the Privacy Act and the fair-information principles that also inform private-sector obligations under the Personal Information Protection and Electronic Documents Act and substantially similar provincial regimes (Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5; Office of the Privacy Commissioner of Canada, 2022). Because immutability can sit uneasily with correction rights and data minimization, procurement ledgers should avoid writing personal data on-chain; instead, they should store salted hashes of documents, with the underlying files held in controlled repositories subject to retention and disposal schedules. Key rotation, revocation procedures, and access logs should be defined in governance documents and referenced in solicitations so that suppliers understand how their information will be processed and how corrections will be handled. This structure reconciles the transparency expected in public contracting with the confidentiality and individual rights that privacy statutes protect.

Governance instruments provide for accountability of automation in procurement. The Directive on the Management of Procurement requires lifecycle planning, risk assessment, and recordkeeping; additionally, where automated decision-making relates to eligibility or evaluation, the Directive on Automated Decision-Making expands with an impact assessment, human oversight, and documentation proportionate to the risk (TBS, 2023; TBS, 2020). In practice, this means to classify each automated rule (such as deadline checks or price-normalization routines) with an impact level, justify the selection, and designate the human decision-maker who will make final determinations in the procurement process. For example, consider a contract where a smart-contract clause automates a post-award obligation, such as the passage (from milestone acceptance) that triggers payment. In that circumstance, the contract should indicate verification criteria, dispute-resolution paths, and a mapping to manual override authority. The simplicity and complexity of smart-contract executions are underpinned by the parties agreed textual rights or remedies; subsequent human agency can ensure it does not go wrong. That is also true for cases where automated eligibility or evaluation (determined by automation) will aid subsequent reviews, such as challenge by a competitor to the Canadian International Trade Tribunal or a practice review by the Office of the Procurement Ombudsman, based on having a record of how automation was configured beforehand and how exceptions were considered afterwards (Canadian International Trade Tribunal, 2023; Office of the Procurement Ombudsman, 2024).

Jurisdictional diversity across provinces and territories shapes deployment strategy. Contract formation, evidence, and many privacy rules are provincial, while federal entities are simultaneously constrained by federal statutes, Treasury Board instruments, and international trade commitments. Cross-jurisdictional procurements—particularly those using shared or pooled buying arrangements—should therefore default to the strictest applicable standard among

participating entities for electronic signatures, evidence retention, and privacy safeguards, and they should memorialize that choice in the solicitation and the resulting agreement. Trade-agreement disciplines at federal and sub-federal levels, including non-discrimination, transparent notice, and domestic review mechanisms, set a harmonizing baseline that any DLT implementation must meet for covered procurements (Canadian Free Trade Agreement Secretariat, 2017; Global Affairs Canada, 2023; World Trade Organization, 2014). This multi-layered discipline reduces forum risk and supports supplier confidence when automation is introduced.

In sum, Canadian law does not preclude the use of distributed ledgers or smart-contract clauses in public procurement; instead, it conditions their lawful use on fidelity to established principles: clarity and fairness in the tendering terms, reasoned and reviewable administration, reliable and admissible records, and privacy-respecting information practices. A pragmatic adoption pathway follows directly from these principles: specify human-readable rules in the solicitation and mirror them in code; implement selective anchoring with robust records governance; conduct impact assessments and assign oversight for every automated step; and design for exception handling and debriefing. Under this model, blockchain becomes a compliance-enhancing instrument that strengthens auditability and traceability without displacing the doctrinal pillars of Canadian procurement law.

Canada's system integrates statutory regulations (FAA, GCR) with tendering common law (Contract A/Contract B) and the Treasury Board Secretariat's life-cycle management mandate. Electronic records are admissible when the standards of system dependability and integrity are satisfied (Canada Evidence Act), but privacy regulations (Privacy Act, PIPEDA, provincial legislation) influence data architecture. Blockchain can encapsulate timing, disclosure, and privilege clauses, although it must maintain rational decision-making and evidential integrity; ledger evidence should be substantiated and elucidated inside departmental records. FAA; GCR; TBS, 2023; Canada Evidence Act; Privacy Act; PIPEDA; prominent cases.

3.5.3. Public Procurement Law in the United States: Legal Framework and Institutions

The United States' federal procurement regime is anchored in the Federal Acquisition Regulation (FAR), a unified body of binding regulations that governs the full acquisition lifecycle for executive agencies. The FAR, codified at 48 C.F.R. Ch. 1, was promulgated under the authority of the Office of Federal Procurement Policy (OFPP) Act and related statutes and is maintained by the FAR Council (Department of Defense, General Services Administration, and National Aeronautics and Space Administration). As an administrative regulation with the force of law, the FAR is issued through notice-and-comment rulemaking consistent with the Administrative Procedure Act and published in the Federal Register before codification in the Code of Federal Regulations (Federal Acquisition Regulation, 48 C.F.R. ch. 1; Administrative Procedure Act, 5 U.S.C. 553).

Substantively, the FAR embeds baseline principles of integrity, competition, transparency, and best value, and it provides the architecture for planning, solicitation, source selection, award, administration, and close-out (see, e.g., FAR Part 7 on acquisition planning; FAR Part 16 on contract types; FAR Part 33 on protests, disputes, and appeals). Competition requirements are grounded in the Competition in Contracting Act, which mandates full and open competition absent a valid statutory exception (41 U.S.C. 3301; FAR Part 6). The regime is further integrated with cross-cutting statutory mandates, including the Small Business Act (15 U.S.C. 631 et seq.) and domestic preference, labor, ethics, and national-security rules that are implemented through mandatory contract clauses (e.g., FAR Subpart 3.1; FAR Subpart 3.104; FAR Part 25).

While the FAR provides a single federal baseline, agency supplements tailor procurement to mission needs and statutory delegations. The Defense Federal Acquisition Regulation Supplement (DFARS), codified at 48 C.F.R. ch. 2, adds defense-specific coverage (e.g., classified acquisitions, export controls, supply-chain security), and the General Services Administration Acquisition Manual (GSAM), at 48 C.F.R. ch. 5, governs GSA-administered schedules and ordering procedures. These supplements must be consistent with the FAR unless a statute authorizes deviation (DFARS, 48 C.F.R. ch. 2; GSAM, 48 C.F.R. ch. 5).

Institutional oversight is multilayered. At the policy level, OFPP issues government-wide procurement policy and coordinates interagency reforms (41 U.S.C. 1101–1131). Ethics and integrity are enforced through the Procurement Integrity Act (41 U.S.C. 2101–2107) and implementing rules (FAR Subpart 3.104), while contractor responsibility and exclusions are governed by FAR Subpart 9.4, Executive Order 12549, and 2 C.F.R. pt. 180. Post-employment restrictions for federal officials are codified at 18 U.S.C. 207, and contractor compliance programs and disclosures are required for larger awards under FAR Subpart 3.10, with potential suspension or debarment for noncompliance (FAR 9.406–2; 31 U.S.C. 3729–3733 for the False Claims Act).

Dispute resolution reflects the system's rule-of-law orientation and offers multiple fora with complementary remedies. Agency-level protests are handled under FAR 33.103. The Government Accountability Office adjudicates bid protests pursuant to 31 U.S.C. 3551–3556 and 4 C.F.R. pt. 21, including the automatic stay mechanism under 31 U.S.C. 3553. Judicial review lies with the U.S. Court of Federal Claims under the Tucker Act (28 U.S.C. 1491(b)), with appeals to the U.S. Court of Appeals for the Federal Circuit. Foundational precedents include Blue & Gold Fleet, L.P. v. United States, 492 F.3d 1308 (Fed. Cir. 2007) (holding that a protester waives challenges to patent solicitation defects if it fails to object before bid submission) and Centech Group, Inc. v. United States, 554 F.3d 1029 (Fed. Cir. 2009) (upholding disqualification for material misrepresentation). Contract claims proceed under the Contract Disputes Act (41 U.S.C. 7101–7109) before the CBCA, ASBCA, or the Court of Federal Claims.

Transparency and performance accountability are operationalized through statutory reporting and integrity systems that contracting officers must consult during award and administration. The controlling authorities include the Federal Funding Accountability and Transparency Act (Pub. L. 109-282) and the Digital Accountability and Transparency Act (Pub. L. 113-101), with related responsibilities implemented through FAR publication provisions (e.g., FAR Subpart 5.3) and responsibility determinations (FAR Subpart 9.1). These legal instruments, rather than agency websites, constitute the authoritative basis for data visibility, integrity checks, and source-selection due diligence.

U.S. procurement law integrates socio-economic policy directly into binding acquisition rules. The Small Business Act requires agencies to pursue government-wide goals for participation by small business concerns, including women-owned, service-disabled veteran-owned, HUBZone, and socially and economically disadvantaged small businesses. These mandates are implemented through FAR Part 19, which operationalizes set-asides, sole-source authorities, and subcontracting obligations, and requires contracting officers to apply the "Rule of Two" when two or more responsible small businesses can satisfy the requirement at fair and reasonable prices (Small Business Act, 15 U.S.C. 631 et seq.; 15 U.S.C. 644(g)(1); FAR 19.5; FAR 19.7; FAR 19.502-2). The 8(a) Business Development Program authorizes sole-source and set-aside awards to eligible firms as part of a remedial, congressionally sanctioned framework (15 U.S.C. 637(a)). In the Department of Veterans Affairs, the Veterans First program gives legal priority to veteran-owned small businesses; the Supreme Court confirmed the mandatory nature of these preferences in Kingdomware Technologies, Inc. v. United States (579 U.S. 162, 2016) under 38 U.S.C. 8127.

Obligations of ethics and integrity pertain to both agency personnel and contractors. The Procurement Integrity Act forbids the revelation or improper use of source-selection information and enforces limitations on employment negotiations and gifts during ongoing procurements, with corresponding regulations in FAR Subpart 3.104 (Procurement Integrity Act, 41 U.S.C. 2101–2107; FAR 3.104). Post-employment limitations for federal officials are established in 18 U.S.C. 207, whereas contractors receiving significant contracts are required to uphold business ethics codes, internal control systems, and prompt disclosure protocols in accordance with FAR Subpart 3.10. False or fraudulent claims incur treble damages and civil penalties pursuant to the civil False Claims Act (31 U.S.C. 3729–3733) and may also result in disqualification from federal contracting.

Contractor responsibility, suspension, and debarment form a preventive integrity screen before award and throughout performance. FAR Subpart 9.1 requires an affirmative responsibility determination, including considerations of satisfactory performance history, integrity, and business ethics; FAR Subpart 9.4 provides the framework for suspension and debarment based on causes

such as fraud, serious performance failures, or knowing violations of law (FAR 9.1; FAR 9.4). Government-wide exclusion authority is reinforced by Executive Order 12549 and the no procurement common rule at 2 C.F.R. part 180. Responsibility determinations are informed by legally mandated information systems: contracting officers check SAM exclusions, consult the Federal Awardee Performance and Integrity Information System (FAPIIS), and review contractor performance histories in CPARS during source selection and award administration (41 U.S.C. 2313; FAR Subpart 42.15; FAR 9.104). These instruments function as statutory and regulatory compliance tools rather than discretionary administrative conveniences, ensuring that best-value decisions are conditioned on documented integrity and performance considerations.

Transparency and data governance obligations complement these integrity requirements. The Federal Funding Accountability and Transparency Act and the Digital Accountability and Transparency Act require standardized publication of award data and related financial information, which agencies implement through FAR publication and reporting provisions (FFATA, Pub. L. 109-282; DATA Act, Pub. L. 113-101; FAR Subpart 5.3). In practice, the legal effect is to embed disclosure and auditability into procurement workflows, enabling ex ante responsibility screening and ex post oversight while reinforcing the defensibility of source-selection outcomes under protest and judicial review.

State and local procurement regimes are established by statute and administrative rule rather than by the FAR, and they typically reflect three pillars: competitive bidding requirements; protest and claims mechanisms; and ethics, records, and open-government constraints. California centralizes state procurement in the Public Contract Code, which prescribes competitive processes, allowable exemptions, and remedial pathways, supplemented by agency regulations for specialized sectors (Cal. Pub. Contract Code). Texas organizes state purchasing in Title 10 of the Government Code, with general purchasing rules and vendor requirements in Chapter 2155 and contract-claims procedures for disputes with the state in Chapter 2260 (Tex. Gov't Code ch. 2155; Tex. Gov't Code ch. 2260). New York's statewide purchasing framework is codified in Article 11 of the State Finance Law, which governs centralized and agency-specific procurements, qualification and award, and contract oversight (N.Y. State Fin. Law art. 11). Many municipalities and special districts follow parallel statutory schemes, often incorporating competitive sealed bidding, best-value selection for services, and limited sole-source authority, while remaining subject to state open-records and open-meetings laws that shape transparency and confidentiality during the solicitation and award phases (e.g., Tex. Gov't Code ch. 552; N.Y. Pub. Off. Law art. 6).

Although state and local entities are not bound by the FAR, federal financial assistance introduces federal procurement standards that operate as a condition of funding. When states, local governments, and universities expend federal grant funds, they must comply with the Uniform Guidance in 2 C.F.R. part 200. The Uniform Guidance requires documented procurement

procedures, internal controls, and conflicts-of-interest rules (2 C.F.R. 200.318), outreach to small and minority businesses and women's business enterprises (2 C.F.R. 200.321), and domestic preference requirements for procurements made with federal assistance (2 C.F.R. 200.322). It prescribes method-of-procurement standards keyed to thresholds and risk, without importing the FAR wholesale (2 C.F.R. 200.320; see also definitions and thresholds cross-referenced in 2 C.F.R. 200.1). It also imposes pass-through oversight duties on prime recipients to monitor subrecipients (2 C.F.R. 200.332) and mandates checks against government-wide exclusion systems consistent with the common rule on suspension and debarment (2 C.F.R. 200.214; 2 C.F.R. pt. 180). In short, federal grant conditions partially harmonize state and local procurements with federal integrity and competition norms while preserving state statutory autonomy outside the scope of federal funds.

Harmonization further occurs through uniform commercial law and model state procurement codes. For acquisitions of goods, state contract formation and performance are generally governed by the Uniform Commercial Code Article 2 as enacted in each state, providing common rules on offers, acceptance, warranties, and remedies that operate alongside public-sector bidding statutes (U.C.C. art. 2). Many jurisdictions also draw on the American Bar Association's Model Procurement Code to structure competitive processes, negotiation authority, and protest procedures, although enactments vary and are authoritative only as adopted by statute or regulation in a given state (Model Procurement Code for State and Local Governments). The practical result is a convergent baseline—competitive methods, written determinations, and defined remedies—implemented through state-positive law rather than federal acquisition regulation.

State-level protests and procurement conflicts are a reflection of judicial and administrative processes that are influenced by sovereign-immunity concepts. For instance, Chapter 2260 in Texas offers limited judicial review upon administrative exhaustion and an exclusive administrative remedy for specific contract claims against the state (Tex. Gov't Code ch. 2260).

Courts also police bidding integrity through state common law and statutory mandates; in a leading decision on public construction, the Texas Supreme Court confirmed that sovereign immunity does not categorically bar equitable remedies for breach when the legislature has authorized suit or where contract terms and statutory schemes contemplate such relief (Zachry Constr. Corp. v. Port of Houston Auth., 449 S.W.3d 98, Tex. 2014). New York's framework couple's agency-level award review with judicial oversight under Article 78 of the Civil Practice Law and Rules, while substantive procurement rules and oversight flow from State Finance Law Article 11 (N.Y. State Fin. Law art. 11). Other states codify analogous structures, such as Virginia's comprehensive statute governing state and local purchasing and protests, including debarment and remedies provisions (Va. Code Ann. 2.2-4300 et seq.).

Finally, federal–state interoperability appears in selective cross-access mechanisms and data-integrity requirements rather than direct regulatory substitution. Congress authorizes certain cooperative purchasing and supply access for state and local governments through federal supply programs, which state entities may use when permitted by state law (40 U.S.C. 502). Even when

states leverage federal supply schedules or grant funds, the controlling legal instruments remain the state's procurement statutes and rules together with the Uniform Guidance conditions and federal eligibility requirements. Across these interfaces, the throughline is legal defensibility: written determinations, contemporaneous documentation, and adherence to enacted procedures provide the evidentiary record that sustains awards against protests and claims, whether reviewed by administrative tribunals or courts applying state and federal law.

The obligations of electronic records and documentation in U.S. procurement are derived from positive law rather than platform policy, and they are binding on both agencies and contractors. The National Archives and Records Administration implements the Federal Records Act's creation, maintenance, and disposition requirements for federal records through detailed regulations regulating electronic records management (44 U.S.C. chs. 31, 33; 36 C.F.R. pts. 1220–1239).

Within the acquisition domain, the FAR prescribes government contract files and retention rules to ensure a contemporaneous, auditable record of planning, solicitation, source selection, award, and administration (FAR Subpart 4.8). Contractor-side recordkeeping and access obligations are addressed in FAR Subpart 4.7, which requires retention of specified categories of books and records and facilitates examination when legally authorized. These authorities, read together, make "digital-by-default" workflows legally sufficient provided they preserve authenticity, integrity, and retrievability for the required retention period.

Digital transaction validity is grounded in enacted e-signature law. The Electronic Signatures in Global and National Commerce Act recognizes that a signature, contract, or other record may not be denied legal effect solely because it is in electronic form, subject to defined exclusions and consent conditions (15 U.S.C. 7001 et seq.). The FAR accommodates electronic commerce by authorizing electronic exchange of acquisition information and documentation when it affords adequate security and integrity (FAR Subpart 4.5). In practice, this pairing allows agencies to issue electronic solicitations, receive electronic offers, and execute awards electronically, while leaving formation and interpretation questions to general federal procurement law and, where incorporated, to state commercial law and common-law principles.

Cybersecurity controls in federal procurement proceed from statute to standards to contract clauses. The Federal Information Security Modernization Act assigns agencies responsibility for risk-based information security, with government-wide standards developed by the National Institute of Standards and Technology (44 U.S.C. 3551–3558). The FAR's baseline clause, FAR 52.204-21, requires contractors handling federal contract information to implement a defined set of safeguarding practices, and agencies may incorporate additional evaluation factors or clauses for systems with heightened risk. Where cloud services are acquired, Congress has now codified the Federal Risk and Authorization Management Program, which standardizes security assessment and authorization for cloud offerings used by executive agencies (FedRAMP Authorization Act, Pub. L. No. 117-263). NIST publications supply the technical scaffolding for these obligations, most notably the security and privacy control catalog in NIST Special Publication 800-53 and the

contractor-focused requirements in NIST Special Publication 800-171 for protecting controlled unclassified information in nonfederal systems (NIST SP 800-53; NIST SP 800-171). Agencies integrate these authorities through solicitation language and contract clauses tied to system categorization and data sensitivity.

Defense procurement adds mission-specific cybersecurity requirements by regulation and clause. The DFARS mandates safeguarding and incident reporting for covered defense information and cyber incidents, including flowdown to applicable subcontractors (DFARS 252.204-7012). To increase assurance, DoD also requires offerors to represent and, when requested, substantiate implementation of NIST SP 800-171 requirements through assessment mechanisms referenced in DFARS 252.204-7019 and 252.204-7020. The Cybersecurity Maturity Model Certification clause (DFARS 252.204-7021) includes a certification framework that DoD could use by rule for defined acquisitions, provided the clause is prescribed, depending on the specific acquisition contract language. Across these forms of acquisition, enforceability is based on regulations and clauses issued as regulatory requirements that are included in the separate regulations, and become binding obligations of performance.

The use of emerging digital tools—distributed ledger systems, smart-contract automation, and AI-enabled procurement analytics—are operating within this established legal structure. As of August 2025, there is no federal acquisition FAR requirement, otherwise generally applicable, for government acquisition with distributed ledger technology or smart contracts; deploying any of these technologies will require reconciliation with any records laws including disposition and transfer, e-signatures, and cybersecurity controls discussed above.

For artificial intelligence, executive guidance has emphasized risk-based governance and procurement discipline without displacing the FAR's competition, responsibility, and documentation rules. Executive Order 14110 directs agencies to manage AI risks and to align acquisition and use with established federal standards and safeguards, while NIST's AI Risk Management Framework provides nonbinding but authoritative guidance on identifying, measuring, and mitigating AI risks in practice (Exec. Order No. 14110; NIST AI RMF 1.0). Consequently, legally sound adoption of automation technologies in procurement turns on orthodox steps—clear requirements, appropriate evaluation criteria, clause selection, and recordkeeping—anchored in enacted statutes, codified regulations, and incorporated standards rather than vendor platform terms or informal guidance.

U.S. procurement is fundamentally record-centric, as dictated by FAR procedures, the Federal Records Act, and NARA regulations, which mandate that decisions be subject to review based on the assembled administrative record (GAO/COFC). Authenticated and cross-referenced blockchain artefacts are valuable components of a record; however, smart-contract automation cannot replace human authorization for changes and determinations. The defensible design maintains canonical documents within records systems, incorporating on-chain attestations

(hashes/timestamps) that are associated with human-readable exhibits and chain-of-custody logs. FAR 4.5, 4.8; Federal Records Act; NARA; GAO/COFC practice.

3.5.4. Comparative Legal Analysis and Discussion

The comparative study of the three jurisdictions of Italy, Canada, and the United States reveals some important structural differences that impact the practicability, legalized usage, and institutional implementation of blockchain technologies within their respective procurement law frameworks. Although all three jurisdictions share the same intent of honesty, transparency, and procedural fairness, they differentiate themselves with respect to their legal culture, enforcement logics, and institutional routes, which in turn inform the use of blockchain as an anti-corruption mechanism. These differences are not only not semantic and academic, but they are structurally different in terms of how smart contracts are understood, how audit trails are internalized, and how data sovereignty and privacy rights interface with the concept of immutability, yet not unknowing. Because of this, an effective legal-comparative study, should not only recognize the differences, but make clear how these differences shape the limits of innovation, compliance, and accountability within public procurement systems.

Italy's public procurement regulations are centralized and codified under the Codice dei Contratti Pubblici, following the EU's legislative order and civil law administrative traditions (D.Lgs. 36/2023). Italian public procurement law favors formal proceduralism, hierarchical control, and ex ante norm compliance confirmation (usually through ANAC and the Court of Auditors). Smart contracts and decentralized blockchain solutions suffer structural limits, notably with automated logic and the lack of a procedural reference in public-contract law governing procurement and contracting.Furthermore, with Italian law not directly recognizing decentralized, self-executing contracts as an enforceable legal instrument, legal enforceability via contract becomes problematic. Also, the interaction with GDPR rights of erasure and rectification pose a tension in the context of blockchain immutability that has not been either addressed vertically in either national case law or EU-level laws. In relation to this tension, as of August 2025, Court of Justice of the European Union relevant case law on erasure and accuracy (including C-507/17; C-460/20) reinforce a strict interpretive obligation and precedence pertaining to a strong privacy ethos that an immutable architecture must comply with (Regulation (EU) 2016/679, arts. 15–17).

In contrast, Canada has a mixed common law regime that is more decentralized, and administratively pluralistic. Federal procurement exists within the structure of the Financial Administration Act, the Government Contracts Regulations, and the Treasury Board's Directive on the Management of Procurement, while provinces have their own legislation to delineate governance in procurement (for example, Ontario has the Broader Public Sector Procurement Directive). For instance, Canada's privacy regime (PIPEDA) has many equivalent principles to the GDPR but is not legislated uniformly across provincial law, which is very diverse and covers the public and private sectors through either separate legislation or decreed statutes. This plurality of

regulations not only permits innovation through pilot programs with ministers having discretion to employ materials like smart contracts, but it also generates legal uncertainty with regard to jurisdiction. As of August 2025, there is not yet anything determinative in case law around evidentiary weight of distributed-ledger records used in public contracting disputes, and no codification of smart contract procurement explicitly, meaning while all of this is technically legally possible; the questions we raised above remain practically unresolved and subject to jurisdictional ambiguity or administrative inaction, and in the case of audit trails vs. automated execution legally tenuous.

The United States has a complex, yet fully developed procurement system, based on the Federal Acquisition Regulation (FAR). The FAR includes a comprehensive legal framework for planning, competition, award, administration, and resolution of disputes, as well as agency supplements (e.g., DFARS; GSAM), and multi-tiered oversight from agency procedures and regulation and the GAO, and U.S. Court of Federal Claims. U.S. law gives legal recognition for electronic records and signatures (E-SIGN Act) and allows electronic commerce in acquisitions (FAR subpart 4.5) - it is important to note that nothing in either the FAR's contract-file requirements, or the rules governing Federal records, addresses blockchain logs as a log; agencies, however must still develop and produce a complete, understandable, and reviewable administrative record that fulfills records-management and evidence-production requirements (FAR 4.8; Federal Records Act; NARA regulations). The legality of accepting cryptographic logs as evidence is, therefore, an issue of inclusion and authentication as part of the complete compiled record, and is not a matter of accepting or rejecting a technology. As of August 2025, there is no general federal rule that expressly treats distributed-ledger records as a stand-in for the administrative record in bid protests or claims.

The question of data sovereignty further differentiates the three jurisdictions in ways that critically affect blockchain's legal integration. In Italy, the interplay between national procurement rules and EU law generates a dual layer of data governance. Procurement records must conform to administrative transparency mandates while remaining consistent with GDPR requirements on minimization, accuracy, portability, and erasure. This yields structural tension for any blockchain using cross-border or consortium architectures. Italian authorities have not issued binding rules on whether hashed on-chain pointers with off-chain storage meet erasure and rectification obligations; thus, designs must prioritize privacy-by-architecture and revocation-capable mechanisms if they are to fit within the GDPR's framework.

Canada has a more fractured but potentially flexible ecosystem. The approach established in PIPEDA allows for a contextual view of emerging technologies. The provinces have their own transparency and privacy legislation; as such, a blockchain pilot project determined to be compliant at the federal level may still have to contend with different provincial requirements regarding record retention, access, and auditability. There is not yet settled case law indicating how far an agency may go to use ledger-based audit trails in procurement disputes, which unnecessarily complicates the dealings of risk averse players regardless of technical viability.

In the United States, blockchain evidentiary status must be viewed with the context provided by FAR documentation requirements and compliance with the Federal Records Act. FAR 4.803 provides an example list outstanding items that are "normally" included in files; however, it is not an exhaustive list. In bid protests and claims, the GAO or the Court of Federal Claims will examine the agency's administrative record to find a reasoned decision, insanity and regularity of process. As such, immutability is of little value unless an authenticated, human-readable, procedurally generated documentation is established as well. The legal value for the purpose of transparency will depend on the accuracy, and provenance, access and compliance with record keeping requirements.

Given that the evidentiary and data governance limitations to inform anti-corruption initiative are profound, ideally Italy's centralized design, however procedurally cumbersome, theoretically layers several positioned governance mechanisms nested within integrity governance structures supported by a ledger—assuming, again, they both respect GDPR-compatible designs and that they have been sanctioned by an authority. Canada's routes to decentralized design support speedy experimentation, and have highlighted inefficiencies in interoperability and misaligned policy coherence. The United States, although it has relatively anchored oversight and disput resolution functions and outcomes, so far does not support the legal operability of blockchain products unless they are represented together with orthodox records-management and source-designation documentation.

The legal enforceability of smart contracts is another dimension of diversity. In Italy, the defined and hierarchical procedures of public procurement complicate the alignment of self-executing performance with the necessities for official revisions, approvals, and certified documentation. No regulatory instrument presently regards code execution as a replacement for administrative actions in public procurement. In Canada, smart contracts align with general contract concepts; nevertheless, there is a lack of procurement-specific codification and adjudication, with manual validations through existing governmental processes prevailing. In the United States, although digital agreements are generally enforceable in private law, public procurement under the FAR mandate’s human-authorized modifications (e.g., Changes clause), debriefings, and secure, documented evaluations—criteria that automated code execution presently fails to meet independently.

Across jurisdictions, the obstacle is not automation per se but the expectation of discretionary review, appeal, and contextual interpretation in public procurement. Smart contracts execute ex ante logic; public procurement embeds ex post accountability and exceptions. Without formal legal pathways that nest automation within existing doctrines—such as conditional admissibility standards for ledger evidence, procurement-specific definitions for code-based modifications, and privacy-conformant record architectures—blockchain adoption will remain peripheral.

Table 5.Table3. 5.4.1 – Jurisdictional Comparison of Legal Constraints and Enablers for Blockchain Integration in Public Procurement

Legal Dimension	Italy (Civil Law, EU Context)	Canada (Common Law, Federated System)	United States (Common Law, Fragmented Federalism)
Legal Recognition of Smart Contracts	Not formally recognized within administrative procurement. Public contracts proceed through codified forms, hierarchical validations, and pre-authorized procedures (D.Lgs. 36/2023).	Permitted under general contract law principles; however, there is no procurement-specific codification or jurisprudence confirming their use in public tenders.	Generally enforceable in private law, but FAR-governed processes require human-authorized modifications and documented procedures (e.g., FAR 52.243-1; FAR 15.506).
Admissibility of Blockchain Audit Trails	Not expressly addressed; centralized, certified records remain the authoritative basis for administrative and judicial review.	Technically feasible but not institutionalized; there is no binding jurisprudence confirming evidentiary sufficiency in procurement review.	Not expressly addressed in FAR 4.8 or NARA rules; acceptance depends on inclusion and authentication within the compiled administrative record (Federal Records Act; NARA regulations).
Data Protection and Privacy Compliance	GDPR governs, including erasure and rectification; immutable architectures must accommodate Articles 15–17 and related case law (C-507/17; C-460/20).	PIPEDA plus provincial privacy statutes apply. Contextual flexibility exists, but uneven harmonization affects ledger design, retention, and cross-jurisdictional compliance.	No comprehensive federal privacy statute; sectoral federal laws and state privacy laws apply. Designs must satisfy records, disclosure, and retention obligations.
Institutional Oversight and Auditability	Centralized oversight via ANAC and Corte dei conti; audits emphasize certified documentation and formally sequenced acts.	Mixed model; federal oversight (e.g., PSPC/TBS, Ombudsman) with substantial provincial variation in audit capacity and rules.	Oversight is divided among agencies, GAO, and the U.S. Court of Federal Claims; evidentiary standards emphasize a complete, reviewable administrative record.
Regulatory Openness to Pilots / Innovation	Constrained by codified mandates and EU-level requirements; pilots must conform to GDPR and	Moderate; departmental discretion and policy directives allow experimentation, subject	Theoretically open, but no express rule treats ledger outputs as compliant administrative records;

	procurement-formalism expectations.	to federal–provincial alignment and oversight.	adoption is contingent on standards and clause frameworks.
Potential for Legal Harmonization	Moderate within the EU context if aligned with GDPR/eIDAS and national reforms.	High in principle but dependent on sustained federal–provincial coordination.	Low to moderate; pluralism across federal/state levels and sectoral silos complicates nationwide convergence.

Notes: Abbreviations—ANAC: Autorità Nazionale Anticorruzione; GAO: U.S. Government Accountability Office; COFC: U.S. Court of Federal Claims; GDPR: General Data Protection Regulation; PIPEDA: Personal Information Protection and Electronic Documents Act; FRA: Federal Records Act; NARA: National Archives and Records Administration; FAR: Federal Acquisition Regulation; PSPC: Public Services and Procurement Canada; TBS: Treasury Board Secretariat. Statements reflect the legal position as of August 21, 2025.

The comparative matrix demonstrates how legal family, locus of administrative authority, and evidentiary doctrine cumulatively condition the admissibility and functional relevance of blockchain artefacts in public procurement. In the civil law environment of Italy, the formal and hierarchical structure of the Codice dei contratti pubblici, along with the oversight powers of ANAC and the Corte dei conti, privilege formally sequenced acts and certified records, rendering self-executing performance and ledger-native logs secondary unless incorporated into positive law and protocols for keeping records. Canada’s common-law, federated structure provide room for interpretative flexibility under general contract law, as well as for authority to be dispersed across federal and provincial regimes; resulting in a space for experimentation but also a lack of procurement-specific codification and jurisprudential anchors for the evidentiary effect of distributed ledgers. In the US, while collections of facts and data output may be neutral with respect to technology, the procurement legitimacy is based on the completeness of the administrative record, and the procurement record is explanatory, producing legal traction for blockchain output only if they were authenticated, human-readable and received as part of a compiled file subject its current record management and protest rule. Across the three jurisdictions, the limiting factor is less about the technical appropriateness of immutability, and more about the legal obligation for procurement decisions to be constructively, contestable, and reviewable in the future with current administrative and judicial forums.

The policy implications are institutional, not purely technological. Italy’s path rests in legislative and regulatory accommodation: e.g., explicit acknowledgment of ledger-natively anchored artefacts as part of the procurement dossier, compliant with GDPR and eIDAS, and with guidance from ANAC aligned with their constructed privacy-compliant informed architecture and revocation-proof designs. Canada's lever for reform is intergovernmental coordination: model

clauses and a common evidential guide have been passed down under federal government words, and if provincial assent could convert permission from pilots to admissibility with the weight of procurement. In the United States, narrowly tuned FAR and NARA updates - specifying the circumstances under which cryptographic proofs, event logs, and smart contract states meet file content and authenticity requirements and entitling their use with the Changes clause and at the time of debriefing - would facilitate automation without undermining due-process-centred procedurally correct values at the protest and claims stage. In all instances, hybrids that retain human authorities with machine execution, and preserve on-chain integrity and off-chain semantics and documentation, offer the clearest path to doctrinal integrity: it retains auditability and accountability while translating the affordances of blockchain into the category of legally operative proof, in the presence of procurement oversight regimes.

These legal divergences dictate whether blockchain can be a meaningful part of public accountability mechanisms. When scrutinized via maps of corruption actor typologies, the effects become apparent. In Italy, where these risks accrue around discretionary variations and opaque formal documentation, immutable and uniquely time-stamped records could deter fraud - so long as these records are before government formalities and formal legal requirements under the identified GDPR, and eIDAS. In Canada, the traceability and audit the blockchain could affect would mitigate interprovincial oversight barriers - somewhere between procurement and privacy. In the United States, the confidence that adversarial oversight will confirm ledger records has limited legal significance relative to the it fits records and protests.

The central intervention of this subsection, accordingly, is to demonstrate that legal structures are not a neutral context; legal structure is a dynamic provision of context determining whether the affordances of blockchain—immutable, automatable, transparent—provide a pathway to anti-corruption ends. Adopting regulatory experimentation, sandboxing, targeted reforms - such as conditionally admissible ledger entries, procurement only definitions of performance from code, and privacy insolvent record architectures - will be necessary for scalable integration. Absent some legal engineering, pilot level projects will remain pilot level and anti-corruption functionally aspirational rather than functional.

3.5.4.4. CPI andWorld Bank analysis

Corruption Perceptions Index (CPI)

Transparency International.

Corruption is broadly defined as the "abuse of power" or "misuse of entrusted authority" for private benefit (Transparency International, 2025). Definitions of corruption include a wide range of practices found across public, private, and civil society for example. Overtly, corruption includes bribery, embezzlement and clientelism; more systemically and less transparent, there's political

patronage, purchasing contracts, and regulatory capture. Corruption also takes many forms and is practiced by agents with diverse roles: politicians can take public money for electoral gain, civil servants can request informal payments for a service to which they are entitled, and corporate actors may collude to influence public contracts through illicit co-ordination. As well, corruption thrives in intermediary professions such as lawyers, accountants, and financiers; opaque governance environments, anonymous corporate structures, and legal enforcement that lacks threat of sanction. As an adaptive phenomenon, corruption has been sustained or not significantly modified by shifting institutional contexts, legal reforms, and technological environments (Transparency International, 2025).

The costs of corruption are also multidimensional, and range from political, economic, social, and environmental costs. Politically, corruption undermines democratic accountability by disrupting electoral competition arena, undermining judicial independence, and diminishing the rule of law. Socially, corruption erodes trust in institutions, separates social actors from a participatory governance role (citizen's role), and perpetuates inequality by providing preferential access to services or opportunities. Economically, corruption distorts the market, reduces investment, and misallocates public resources that are essential for inclusive development. Environmental harm is associated with corruption, particularly the discretionary use of regulatory roles to award licensing rights, establish land uses and exploitation of resources (Transparency International, 2025). Transparency is a necessary first step; but if governments, civil society and the private sector institutionally collaborate necessary to curb corruption, challenges to corruption can only emerge in time through the use of good data and appropriate tools including the use of both the Corruption Perceptions Index (CPI) and the Global Corruption Barometer (GCB) to use one or both of these tools to understand the scale, scope, and perceptions of corruption across institutional settings (Transparency International, 2025).

Table 6.CPI Scores (2015–2024): Italy, Canada, and United States

Year	Italy	Canada	United States
2015	44	84	76
2016	44	81	74
2017	47	81	75
2018	47	78	71
2019	50	75	69
2020	52	75	67
2021	52	75	67
2022	53	75	69
2023	53	75	69
2024	56	75	65

To contextualize the legal and technological realities for blockchain-based institutional anti-corruption measures in public procurement, it is important to consider how institutional perspectives of corruption have changed within the jurisdictions of analysis. The Corruption Perceptions Index (CPI) published annually by Transparency International provides a standardized global metric for longitudinal examination of public sector integrity. The CPI is scored from 0 (highly corrupt) to 100 (very clean) and is derived from expert assessment data and business survey data. Although the CPI does not score measured incidents of actual corruption, it scores perceived levels of corruption and, as such, is a significant facet of institutional variables that affect institutional trust, policy uptake, and governance innovation. The 2015 - 2024 data for the US, Canada, and Italy (see Table: CPI Data 2015 - 2024) revealed three main institutional trajectories which have implications for the adoption and credibility of blockchain corruption interventions in public procurement.

Comparatively, Canada scores the highest CPI scores during the full ten-year period, starting in 2015 at 84 and bottoming out (i.e., stabilizing) at 75 by 2024. While not a significant collapse, the decline is 9 points, and Canada still presents as a high-integrity profile that is at or above the world average. The overall decline is not insignificant, while it is mild, it does indicate some level of decline in perceived accountability and trust.A number of contributing factors mentioned in the academic and policy literature have been issues around lobbying-related scandals, the concentration of procurement, and concerns over the oversight of emergency contracting as a result of the COVID-19 pandemic. Notwithstanding factors affecting Canada's moderately declining CPI baseline, Canada, as a jurisdiction still clearly has a relatively strong base of institutional performance and a solid legal framework, and is generally a better country to pilot blockchain-based reforms to procurement. For instance, ongoing e-procurement practices combined with federal transparency requirements (for example, proactive disclosure under Access to Information Acts) denotes a more enabling context for digital governance. The gentle decline in CPI does not show what appear as system estimated failures; but, rather from pressures to uphold high quality governance amidst growing complexity and public expectation.

In contrast, the most serious reduction in perceived integrity in the public sector has occurred in the United States. The CPI score fell from 76 in 2015 to 65 in 2024; an 11-point drop over that ten-year period. The momentum behind the decline combines various aspects of institutional, political, and legal factors, including, increased polarization; politicization of oversight institutions; inconsistently applied federal laws regulating procurement; and scandals involving high-level lobbying and corporate capture as well as practices involved in opaque emergency contracting have negatively impacted accountability. To add to the complexity, the federal character of the United States means wide variation across states in terms of procurement rules, transparency mandates and adopting digital tools. Many states have explored some progressive blockchain pilot initiatives (e.g., Vermont, Wyoming), but the larger trajectory at the national level indicates regulatory fragmentation, with the increasing perception of eroding public confidence. This trend was particularly meaningful for blockchain integration. While the United States private

sector remains a global leader in technology development and innovation, declining CPI does not signal a logical basis to assume that there is the requisite political or legal interest related to embracing systemic blockchain as a means of novel public contracting, as there are likely significant legal impediments as it relates to the enforceability of smart contracts; data privacy concerns - especially in the absence of a federal GDPR-like law; and procurement audits.

In contrast, Italy has exhibited a steady upward trajectory for CPI scores, from 44 in 2015 to 56 in 2024. This 12-point increase demonstrates genuine institutional measures to endorse anti-corruption mechanisms, especially in the area of public procurement. The formation and beginning of operations of the National Anti-Corruption Authority (ANAC); the digitizing of procurement platforms (like the BDNCP or OpenCUP); and compliance with procurement regulations under the EU regime have all contributed. While Italy still wrestles with significant existing conditions, such as entrenched regional differences across Italy, pervasive clientelism associated with subnational governance, and excessive and complex administrative layering, the rising CPI trend shows that Italian civil society, as well as the compliance professional academy and experts recognize the success of various methods of making institutions more credible versus suspect. Broken down into temporal contexts, the rising CPI trend appears to coincide with discussions for blockchain pilots in public procurement (food traceability and contract registration). The CPI trend from Italy supports the argument that systemic perceptions (or at least continuous improvements in perceptions) of integrity would create a greater amount of institutional willingness to experiment with trust-based technologies, like blockchain. However, since the CPI summarizes only perceptions and not outcomes, it is important to mediate the perceived improvements with actual audits of implementations and legal performance to determine whether the systemic reforms have caused a genuine shift in the dynamics of corruption or merely recast the paradigms for discourse.

When considered holistically, the three jurisdictions revealed anti-corruption trajectories that were in stark contrast to each other that operated in tandem with three distinctive institutional conditions. The relative stability and consistently high level of CPI (with a minor decline) in Canada must be framed with a view of mature governance systems under incremental pressure. The United States continues to have an unrivaled ability to innovate, yet the decline on perceived control of corruption pattern also indicates backsliding in the institutions existing governance structure that is not insulated from legitimacy impact or possibly disrupt/reduce legitimacy for political continuity in, either with technology reforms, either as bureaucratization or legal regime decisions that coalesce political coherence. The progressive increase in Italy demonstrates the proquest of institutions towards reform; however, their point total on average is significantly lower than that of both Canada and the United States and there remain vestiges of conditions that could deny conclusion in a transition towards technology lead governance if the conditions are not addressed. The systematic comparative motion patterns provide a priest typology of an internal structure that could guide how potentially blockchain-based anti-corruption tools could be received and calibrated as both deterrents, continuums of accountability or co-opted institutionally.

The CPI trends provide further, methodological affirmation that the designers made the right methodological choice to include descriptive quantitative data alongside the legal analysis of a document-based study. For example, Italy's increase sti1l occurred alongside a growing number of regulatory documents that have emerged in order to explore ideas like transparency or digital integrity however; Canada with its increase but smaller relative decrease raises questions, given the long presence of established regulation on procurement, about substantive impact. The downward trajectory of corruption control is consistent with the years of substantive efforts to roll back regulation, politized institutionalized actions, the impacts of political discourse around sidelining on independent institutions in America during forensic document studies. These tendencies are by no means deterministic; however, they do provide an evidence-based layer of analysis for triangulation and provide usable reference points for structure of institutional policy discourse. As a context variable, the CPI, has the advantage of being able to also offer useful point indications for public sector opacity, legal misalignment, or even a warning to governments with the risk of, "over subscription to emerging technologies".

To sum up, the examination of CPI scores from 2015 to 2024 demonstrates the importance of thinking about technological solutions as existing within an overall web of institutional trust and levels of governance performance. Each jurisdiction represents a unique trajectory of anti-corruption effort shaped not only by historical legacies, legal justifications, and changing political economies. The findings in the previous chapters strengthen the claim that blockchain’s potential role as an anti-corruption measure in public procurement is not uniform, but dependents highly on jurisdiction-specific governance trajectories and the aura surrounding them. Including CPI trends of the jurisdictions adds empirical depth to the legal–technological analysis in a comparative perspective, thereby reinforcing the empirical robustness of this dissertation’s evaluation of the potential of blockchain technology to address corruption.

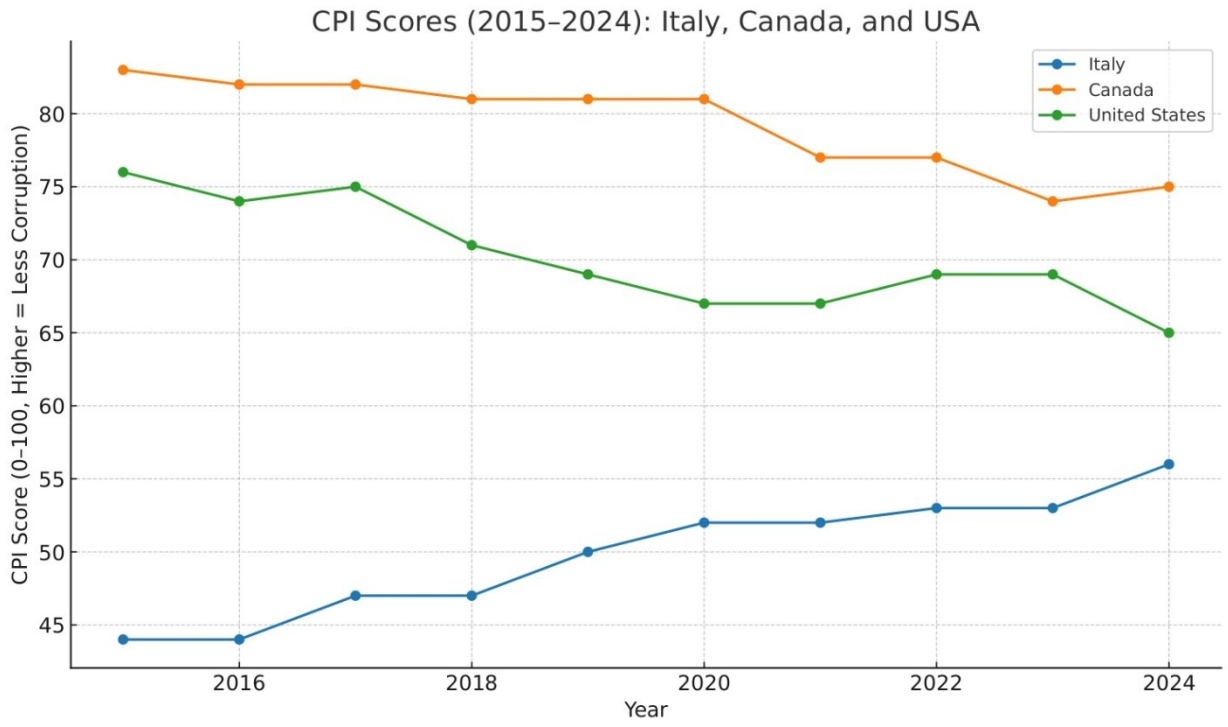

Figure 3.CPI Scores (2015-2024):Italy,Canada,and USA

Comparative Evolution of Corruption Perceptions (2015-2024): Institutional Contextualization Across Jurisdictions

An analysis of Corruption Perceptions Index (CPI) trends over the 2015–2024 timeframe provides an evidence base for evaluating the institutional contexts in which the adoption, resistance, or consolidation of blockchain reforms for public procurement occurs. The consideration of the CPI scores from Transparency International for each year reviews CPI changes not only in public sector integrity across Italy, Canada, and the United States, but also to normative trajectories in institutional trust, rule of law, and administrative transparency—well-grounded dimensions that are relevant to blockchain adoption as an anti-corruption measure. The CPI is a composite indicator of perceptions, not an objective measure of incidents of corruption, and aggregates assessments of expert and business respondents from multiple validated sources. However, the consistency of the CPI and the ability to evaluate cross-nationally makes the index an indicative interpretive frame in legally-oriented governance analysis, especially when referring to qualitative legal-regulatory evidence.

The observed path of Italy's CPI scores over this decade demonstrates a slight but consistent elevation score from 44 in 2015 to 54 in 2024. Therefore, over the ten-year period, Italy's CPI scores improved by 10 points, indicating a perceived steady increase in integrity in the Italian public sector, even with concerns regarding procurement secrecy, clientelism, and the uneven enforcement of the anticorruption regulations by pertinent regions. The upward trajectory aligns with Italy's institutional reforms related to the 2014–2016 anticorruption reforms, the

establishment of the Open Data Portals through the National Anti-Corruption Authority (ANAC), and the digitization of the oversight market for procuring authorities through the OpenCUP, and subsequent BOONAP and OpenCUP system. However, the data need to be interpreted cautiously due to Italy's ongoing structural limitations such as bureaucratic fragmentation, the differing legal origins of regional jurisdictions, and the continuing strength of legacy administrative cultures, all of which inhibit full institutional convergence to the EU-wide transparency standards.

Therefore, the increase in CPI levels may represent subjective optimism related to discursive institutional innovation rather than an effective change of practice.

In contrast, Canada's CPI trend demonstrates a period of perceived institutional stability and minor regression since their peak. Canada experienced an integrity profile well within the moderate range, showing scores of 81 to 84 from 2015 to 2017 in line with its reputation for effective oversight, transparent procurement systems, and whistleblower protections. However, starting after 2018 the CPI plateaued and then gradually declined, returning to a score of 75 in 2024. Although Canada remains one of the top performing countries in the Americas region, the minor downward trend may relate to high publicity procurement scandals, questions about lobbying transparency at the federal level, and increasing scrutiny surrounding indigenous contracting policies and supplier diversity mechanisms. The downward trends do not necessarily represent systemic corruption rather shift towards increased public expectations of equity, inclusivity, and digital accountability in state-market relations. For this dissertation, Canada's relatively high, albeit declining, CPI profile provides a complex context: a jurisdiction with established elected governance systems subject to emergent risks and pressures for legitimacy in relation to the digital procurement space and accountability systems associated with blockchain.

The United States, historically known as a world standard for regulatory enforcement, experienced the largest decline of any of the three case jurisdictions. The CPI from the United States decreased from 76 in 2015 to 65 in 2024, which is an 11-point decline.The nearness of dissimilar trends was accompanied by institutional disruptions, declining federal trust, politicized procurement reforms — most significantly during 2016 - 2020, and most pertinently, for perceived loss of integrity reasons, many of the evident issues appear to be the result of compound factors such as state level regulatory program fragmentation, legal uncertainties related to lobbying practice, and various large-scale procurement scandals about emergency contracting involving defense contractors, pandemic era emergency procurement, and fossil fuels industry subsidies. Further, a host of high-profile corporate corruption scandals surrounding public officials, lobbying capture, and other abuses of trust has complicated the condition of procurement governance and integrity even if the law is dormant. For blockchain integration this presents a contradiction; while the U.S. is at the centre of technological worlds -- and the private sector is often second fastest to define and consider new technological readiness -- the federal-state fragmentation, downward CPI trends, and institutional ambiguities present actually coherent structural and institutional risks for disclosure, structural, legally coherent integration of trust technologies relevant to systems of procurement.

When looking collectively at CPI trajectories there are signs that while these three countries uphold liberal democracy as governing systems, they are each pursuing distinct trajectories of thought in what corruption constitutes in their respective national contexts that ultimately informed the legal parameters, political will and policy framework to advance blockchain-supported procurement reform through transparency-enhancing technologies within a system bound tightly to jurisdictional discretion, political lobbying, and administrative regulatory understanding and acceptance.

The CPI data represents; methodologically the data is not direct evidence of corruption, but a context for communicating mapping the qualitative document analysis outlined later in this dissertation. For instance, where we assess the stated functions of a regulatory policy document or pilot program in a jurisdiction within a year of shave of declining CPI score, any assessment of its supposed efficacy, and knowledge of its reception must also be considered within this context of reduced institutional trust. Conversely, where CPI scores increase after implemented e-procurement reforms or processes, and started from an openness of the contracting process--including the trajectory of Italy after 2016--it might signal an period of significance for policy development or some open opportunity. In this way, CPI trajectories did provide a way of diagnosing and triangulating where institutional conditions, procedural justice and public legitimacy were in place or around what to in a meaningful way implicate in comparisons.

Overall, the CPI trend analysis conducted during the flowering of the 2015-2024 licensing of technical means of conducting public procurement either supports/discredits the principal claim of this dissertation that the formal configuration of blockchain is not merely a matter of procedural justification--technical feasibility--but considerably constructed by the governance settings, historical trust patterns and legitimacy of the policies it attends to. This project was carefully devised to have the comparative analysis of CPI trajectories as a frame so that the legal repository and technical analysis could be rich with observations of the observable dynamics of institutional integrity and embedded rotating door reputational reform. In this way, CPI data provides the necessary caution and prospects for reminding us that technology per se, cannot supplant systemic reform as an alternative, but under enacting technical governance conditions could homeopathically provide the causal touchpoint for reframing reform.

World Bank Analysis

Quantitative Governance Trends in Italy (2015-2023): A Longitudinal Assessment of Institutional Politics for Blockchain-Enabled Anti-Corruption Strategies

Understanding Italy's governance indicators over the last ten years reveals the dynamics of the systemic issues of governance and possible governance changes that are contextually relevant to the technological modernization of risk-free public procurement systems. This understanding of time is vital for assessing the potential and contextual conditions for the integration of blockchain as an anti-corruption intervention. The four indices encompass Control of Corruption, Government

Effectiveness, Regulatory Quality, and Rule of Law between the years of 2015-2023, and we apply standardized estimates from the Worldwide Governance Indicators (WGI). Each of these indicators can constitute both theoretically and operationally significant preconditions for blockchain adoption in the public sector in situations where there are legal enforceability, institutional capacity, and trust in the fairness of the process when applying innovation in a digital context.

The most distinguished governance change is reflected in Control of Corruption index. Italy's improvement from 0.03 in 2015 to 0.55 in 2023 is nuanced over time, with the most substantial change recorded from 2019 to 2020 (0.23-0.51). The pivotal moment occurred when there was formal national and EU political attention directed toward digital transparency and modifications to e-public procurement. The timeline for this change also coincides with Italy complying with the European Commission mandates for seamless, interoperable public procurement systems. The elevation from 2021 to 2023 leads us to believe the context is conducive for embedding technological integrity mechanisms, such as blockchain and audit trails.This finding illuminates that, as with both indicators discussed above relating to societal readiness and the public sector capacity, blockchain has a greater opportunity to facilitate successful innovations in public procurement, where institutional anti-corruption and governance capacity begins to take root. Here blockchain is less a correction or compensatory mechanism to deal with the dysfunction of specific regimes, rather it appears as a midrange layer for change in situations where governance is not being built up, rather it may be complemented.

Conversely, Government Effectiveness indicator showed a less systematic approach to outcomes. In Italy, the value peaked at 0.54 in 2016, declined to 0.36 in 2020 then climbed to 0.61 in 2023, suggesting that Italy still is in a tumultuous and less stable environment in terms of public sector management, administrative capacity, and effectiveness or efficiency of service delivery, all are important for the integration of digital systems. The climb after 2020 may be due to Italy's efforts to develop and significantly invest in public administration and digital infrastructure, aided by pandemic-based development opportunities and funding mechanisms provided under the EU Recovery and Resilience Facility. However, in highlighting the lack of temporal consistency highlighted by the dislodging of a direct relationship between political will, funding and digital procurement reform and the success of the reform payouts, speaks to the importance of sustained capacity and collaboration among agencies. Any deployment of blockchain cannot be considered a piecemeal undertaking and has to have sound implementation governance along with, an orientation to develop pilots, build capacity, legal-technical harmonization, to mitigate the risk of obsolescence and disjointed implementation.

In addition to... above variables, the Regulatory Quality indicator fielded marginal implications which is important to identify the normative context in which blockchain technologies are enabled or either disabled. Italy exhibited significant variations in the Regulatory Quality indicator from 2015 to 2023, (2020 = low = 0.49; 2019 = high = 0.94; and in 2023 = 0.64). The debt-from-average non-linear standard deviation observance from 2015 to 2023 exposes tensions identified between regulatory ambition and systemic capacity to defend and sustain reform. As articulated, the high

observed in 2019 coincided with the most policy experimentation about public sector digital innovation and modernization, e.g. regulatory sandboxes, and as most of first phase external development efforts involving digital identity systems. The subsequent decline in the 2020 evidences emergency COVID-19 regulatory actions, where emergency governance would have likely deprioritized agendas about long-term, sustainable digital transformations. The increase thereafter may suggest a refocusing of the regulatory area, but the discussion arouses concerns and questions about how Italy will be able to secure, maintain and/or sustain a steady regulatory trajectory that will be viable for continued innovation through 2023. Indeed, for blockchain implementations in public procurement, regulatory quality is required not only to legitimize new technologies based on enabling statutes, but oversee risks via regulation and legislate tech standardizations to manage - i.e. for decisions about interoperability, data requests, and enforce approving controls on smart contracts. Finally, in the context of the Rule of Law, Italy shows a weaker and more fragile institutionally based story. Scores for Italy tracked between 0.21 in 2020 to 0.39 in 2023, with erratic year-to-year changes and no sign of systemic improvement. This relatively low and volatile outcome is especially concerning for blockchain-based anti-corruption reforms, because the viability of the rule of law is the enforceability of signed contractual obligations of procurement, legitimacy of the audit trail, and the rights of all parties to procedural fairness in public tenders. The anticipated features of blockchain provide immutability and non-repudiation, but are seriously diminished in non-judicially efficient, guaranteed access to a remedy, or non-predictable administrative systems. This supports the hypothesis that blockchain efficiency is positively correlated, not only to how technologically mature the system and regulations are, but also to how accessible the legal ecosystem is to absorb and adjudicate these digital processes. In Italy, any meaningful use of blockchain as a form of procurement must deal with the structural limitations in the legal system, perhaps through parallel reforms like digitizing court recordkeeping and modernizing administrative justice systems and legal intelligibility around acceptance of smart contracts.

Overall, Italy's governance profile across the 2015-2023 timeline suggests a more mixed, but generally improving environment for blockchain-enabled public procurement reform to take place. The generally greater than the pre-existing trajectories of corruption control, and the rises in government effectiveness are inherently positive indications. A further caution is warranted due to the odds and cyclical nature of regulatory quality (and then rule of law as a structural indicator), meaning that blockchain cannot be adopted naively or without some level of caution in a systematic staged process. These findings reveal the embedded complexities and significance of imbedding the technological opportunity into a structured institutional reform process—one that converges the legal enforceability of the agreement, the regulatory horizon of the agency, and the degree of administrative competence of the processes, as co-dependent elements in the successful use of blockchain.

Table 7.Table 3.5.4.4.1. Italy – Governance Indicators (2015–2023)

Indicator	2015	2016	2017	2018	2019	2020	2021	2022	2023
Control of Corruption: Estimate	0.026578	0.081555	0.175231	0.215687	0.233935	0.509536	0.517085	0.527714	0.550129
Government Effectiveness: Estimate	0.490197	0.544245	0.491924	0.408853	0.450930	0.360755	0.325261	0.448645	0.611037
Regulatory Quality: Estimate	0.712537	0.697885	0.691279	0.715148	0.942924	0.487741	0.526739	0.510931	0.644032
Rule of Law: Estimate	0.288354	0.366415	0.319134	0.240624	0.272417	0.206683	0.240348	0.296974	0.390359

Note. Data from World Bank (2023). Worldwide Governance Indicators. Standardized governance estimates range from −2.5 (weak) to +2.5 (strong).

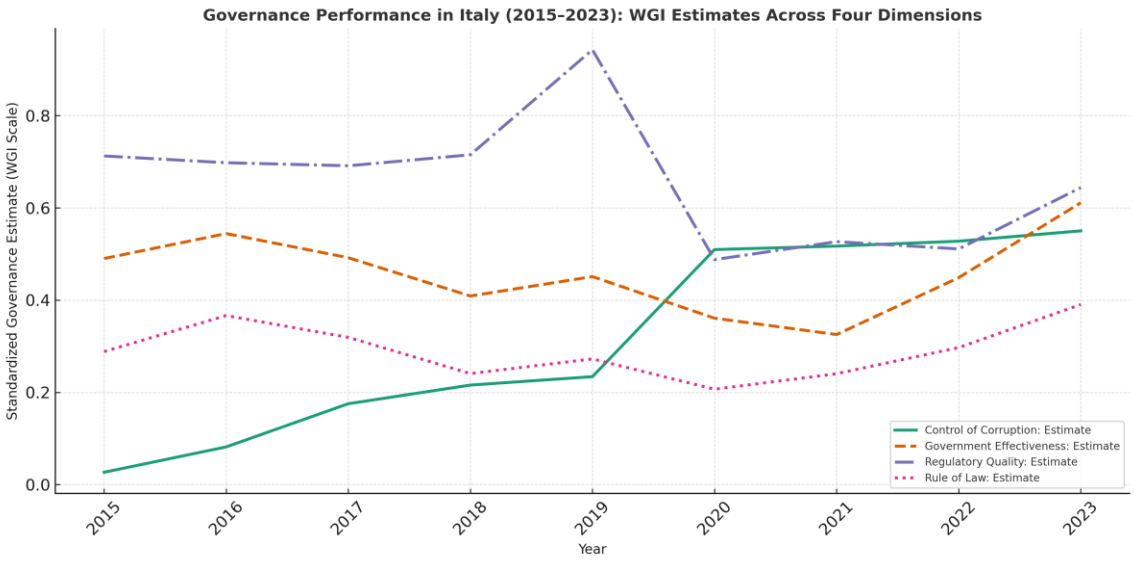

Figure 4.Figure Governance Dynamics in Italy (2015–2023): A Longitudinal Visualization of Institutional Preconditions for Blockchain Integration

This figure provides a chronological overview of Italy's governance capacity in four key institutional indicators: Control of Corruption, Government Effectiveness, Regulatory Quality, and

Rule of Law. These indicators are relevant to measuring a country's able condition for taking on complex governance innovation through a digital governance strategy; that is to say, government procurement for complex digital innovation that includes the implementation of blockchain technology into the National Anti-Corruption Authority (ANAC) digital monitoring. The data information is from the World-Wide Governance Indicators (WGI) collection of datasets from the World Bank. WGI gave insight into a multi-indicator view of governance-based Italy, focused particularly in 2015 to 2023 defined by some level of political transition, deregulation, and technology in governance modernization.

The Control of Corruption line (the darkest blue line in the representation) demonstrates a discernible upward slope and is particularly salient as the indicator increased from 0.03 on a -2.5 to + 2.5 scale in 2015, to about 0.55 by 2023. This upward slope commits the notion that the progress reflected enhanced Italy's abilities to prevent the misuse of public office for private gain either through an increase in enforcement, or more significant changes to its administrative practices. The upward slope is greatest between the years of 2019 to 2020, suggesting a possible inflection point dictating a need for policy change that was conjunctively provided a mandate by the EU directives for digital transparency in governance, and representational emphasis of monitoring and as a measure of effectiveness of one of its mandates by ANAC respectively. Collectively, the data supports a possibility of increasing positive gains as supportive evidence of a governance context that will support designing permanent systems of audit and get transparency to be role-based, two functions of blockchain.

By contrast, the Government Effectiveness curve shows a significant amount of oscillation or variance. Beginning with an initial high in 2015 (0.49), it moves slightly upward in 2016 (0.54), before sharply declining (to 0.32 in 2021) and recovering in 2023 (0.61), which was the highest of all years. While this high reflects considerable variation in public sector performance, periodic instability in administrative coordination and, perhaps, discontinuities of political accountability in the appointment and removal of public administration leaders, it is important to note that the recovery from the minimum coincides with significant post-pandemic public investment in Digital public services, as well as e-procurement modernization, particularly as part of the EU Recovery and Resilience Plan. Moreover, the diminishing curve supports the idea that implementation options and considerations are fragile. For blockchain to be institutionalized and not just token, the public sector must exhibit not only effectiveness but sustained effectiveness that supersedes the temporary.

In addition to a minor resurgence in 2019 (0.94, and the annual high), following below-average values and trends in Regulatory Quality (around 0.64 in 2023), the pattern is non-monotonic. The 2019 peak may have occurred at a time when Italy was engaging with significant digital governance reforms (open-data mandates; interoperability frameworks). The drop from 2019 to 2020 coincides with, inter-state governance moves coinciding with the COVID-19 pandemic, which, with some level of reasonable inference, may involve either potential regulatory congestion, including either consensus-seeking in the courts, or legislative redirection, or perhaps

risk aversion in issuing new normative instruments of accountability and co-ordination as new uncertainties surfaced. The subsequent recovery may imply that Italy is working to return to a regulatory trajectory with progress possible in respect of developing capabilities for oversight, governance, and ultimately innovation as a superseded capacity, responsiveness raises important questions about institutional resilience and regulatory continuity, both of which are important features to law when developing blockchain applications, including attribution, legal certainty and accuracy.

The line representing the Rule of Law remains lowest and most unstable of the three indicators during the periods measured. Following a brief resurgence in 2016 (approx. 0.38), the trend line continues to decline, reaching a low in 2020 (primarily under 0.21). While recovery toward 2023 (0.39) completed, it is noteworthily repeatedly below average to include potentially recessionary trends, with potential structural shortcomings with respect to Italy's legal system, whether it is legal antibiotic, enforcement and reliability of; based capacity, or legal clarity for legal proceedings. For blockchain-enabled procurement reformation, particularly engaging smart contracts and digital evidence, and algorithmic adjudication, and any reliance on legally-engaged supplementary process, recourse to legal measures is essential to integrity and predictability. The pre-secure mechanisms rely, both, on complimentary judicial and legal modernization and harmonization, otherwise blockchain may be a parallel system with little interoperability across legal/operative frameworks for legal assessment and none-existence across other legal orders.

Figure 6.1. Governance Performance in Italy (2015-2023).

Governance Trends in Canada (2015–2023): Evaluating Institutional Stability and Implications for Public Procurement Reform Cannot One Decision or Action at a Time for Blockchain Adoption.

Canada’s governance performance during the period of 2015–2023 shows evidence of a path characterized as having relatively high institutional baselines but increasingly evident downward trends particularly in the administrative performance and quality of legal dimensions. This evaluation employs the World Bank’s Worldwide Governance Indicators (WGI) data, standardize estimates to analyze four core governance dimensions - Control of Corruption, Government Effectiveness, Regulatory Quality, and Rule of Law serve as proxies for exploring the country’s institutional readiness to adopt blockchain in public procurement. Given more volatile governance contexts, Canada’s consistently higher than expect scores across all four dimensions offer evidence of a system that generates higher institutional capital. However, the perceived declines post 2019 can seriously question systems momentum and governance coherency for governance reform in relation to both digital innovation and corruption control.

Canada’s Control of Corruption score starts at a global high of a score of 1.85 in 2015, reaches a high point of 1.94 in 2016, and declines to 1.67 in 2023. While still well above, the OECD average,

the decline and particularly the drop from 1.73 to 1.57 between 2019 and 2020 suggests growing public sentiment avoiding elite accountability, the rise in federal ethical violations, or lesser perceived transparency in procuring oversight. In terms of blockchain, the institutional infrastructure appears to remain strong, but a potential decline in perceived integrity could encourage societies to invest further in technology for a tamper-evident, decentralized ledgers for procurement. In increasingly high-capacity social systems, blockchain is not considered compensatory but as a transparency experience reinforcing the foundation for anti-corruption governance while increasing auditability and public trust.

The Government Effectiveness indicator represent a similar downward trend. From a high score of 1.82 in 2017, the scores move point downward to 1.52 in 2023 and show declines after 2020, suggesting some kind of quality effect on either public service, in policy implementation or bureaucratic efficiency. Canada has historically ranked among some leaders in global best practice public administration, however the cumulative drop in score points across all eight years, may be evidence of systemic fatigue and difficulties accounting for intergovernmental digital policy co-ordination or systemic exhaustion from pandemic response priorities. With blockchain, being able to eventually integrate planned procurement into workflows, especially in perhaps federally constructed/provincial share environments, consistent government effectiveness will be required. The declines in the effectiveness indicator factors will likely introduce frictions in planned cross-jurisdictional platform adoption, increase resistance to the appropriation of smart contracts, or delays in harmonization of procurement standards required for interoperability. The Regulatory Quality indicator, despite maintaining relatively high absolute values across all years in the period of interest, has also steadily decayed overall. Regulatory Quality falls from 1.88 to 1.64 from 2017 to 2023. The lowest point is in 2020 (1.59), which seems to correspond with the stress of the COVID-19 emergency governance response and regulatory reorientation. There is a slight recovery in 2022, but the overall decline is worrying because it may signal limits to a forward thinking and innovation facilitating regulatory environment. Regulatory quality is an especially important variable for blockchain-based reforms in procurement: smart contracts, distributed ledger technologies, and public key infrastructures must have flexible and ongoing regulation. That said, formal regulatory recognition of new digital tools is generally contexts that favor high regulation. However, if the aforementioned decay trend is valid, there may be delays associated with regulatory processes, legal uncertainty, or ongoing fragmented approaches to standard setting through agencies. Under these conditions, the inconspicuous institutionalization of blockchain in procurement could prove difficult unless governments take aggressive action to advance the public management of digital governance arrangements.

The Rule of Law dimension in Canada equally demonstrates an overall declining trend, although it continues to be relatively strong at an international level. The indicator fell from a peak level of 1.81 in 2015, to 1.47 in 2023, with greatest decrease post 2019. Again, this decline, while limited may reflect increasing legal complexity in intergovernmental relations, competing claims to jurisdiction over digital transformation, or growing public interest on the algorithmic governance

and attendant accounts behind law. Whatever the contextual situation is regarding overall market frameworks for blockchain deployment in public procurement, the rule of law underpins important institutional assurances including 1) enforceability of smart contracts, 2) right-based procurement appeal processes, and 3) legal recognition of the cryptographic integrity of transactions. A useful precariousness in the rule of law, seems not to indicate a breakage of the legal system, but raises questions on how clearly a legal framework able to adapt to contemporary and future developments, would support the deployment of modern and cutting-edge digital tools. The disconnect of the operational logic of blockchain from Canada's administrative jurisprudence creates open spaces for legal ambiguity, particularly in the areas of federal contracting law and data sovereignty.

To conclude, Canada's governance trajectory over the last decade illustrates contradictory realities: while Canada has a relatively strong institutional environment, the data shows a consistent decline across all four key dimensions of governance and are troubling across all areas. The data, however, suggests that while Canada is in a non-disadvantageous position relative to other jurisdictions to encourage blockchain turnover in public procurement, the momentum requires upfront and aggressive management to in complacently realize the execution of blockchain projects. While there are jurisdictions where blockchain is being used to minimalize governance gaps, Canada's unique challenge is incorporating blockchain-like surrounding technologies into the historical centralization of institutions, which allows to manage risk in discipline, while maximally increasing transparency in procurement and preemptively manage centralization-induced legitimate or illegitimate disaggregated pathways. This would demand not just digital readiness, but contemporary obligations to responsive regulation, intergovernmental engagement, and clear judicial responsibility - all the accoutrements that accompany importing de-centralized technologies into a regulatory system designed from inception, on the centrality of federal authentication and administrative law.

Table 8.Table 3.5.4.4.3: Governance Indicators for Canada (2015–2023)

Year	Control of Corruption: Estimate	Government Effectiveness: Estimate	Regulatory Quality: Estimate	Rule of Law: Estimate
2015	1.846	1.731	1.706	1.807
2016	1.944	1.745	1.727	1.801
2017	1.881	1.816	1.880	1.763
2018	1.790	1.675	1.699	1.715
2019	1.730	1.697	1.710	1.720
2020	1.566	1.598	1.593	1.619
2021	1.616	1.561	1.614	1.593
2022	1.659	1.567	1.677	1.565
2023	1.672	1.517	1.645	1.473

Note. Data from World Bank (2023). Worldwide Governance Indicators. Standardized governance estimates range from −2.5 (weak) to +2.5 (strong)

This diagram presents a longitudinal visualization of Canada's governance performance from 2015 to 2023, measured through four standardized indicators, taken from the World Bank frequently cited dataset of Worldwide Governance Indicators (WGI): Control of Corruption, Government Effectiveness, Regulatory Quality, and Rule of Law. The measures in Figures 2–5 are on a normalized scale, which is essential for making a comparison of Canada's institutional stability over time, including detection of comparatively narrow, but meaningful movement in governance functions for which public procurement relies upon inferences on blockchain reforms' feasibility and logic in their sustainability.

In the first instance, the figures reaffirm that Canada consistently occupies a high-governance band, with scores for all four indicators between 1.47–1.94 across the nine-year reporting period. Although each indicator demonstrates institutional robustness in Canada, which has served Canada tremendously as an enabler of increasingly sophisticated digital transparency mechanisms, the trend shows a slow but iterative decline across all four indicators after their respective highs between 2016-2017. This change is particularly pronounced in Government Effectiveness and Rule of Law, which are both descending towards flat-line status up until 2023. This trend does not characterize a failing institution, but do suggest cancelled administrative receptivity, deteriorating societal confidence in legal accountability, or persisting frictions in intergovernmental coordination - which is especially consequential in federated governance contexts.

The most observable post-2016 descent appears to be from the Control of Corruption line which falls from a high of 1.94 in 2016 to a low of 1.67 in 2023.While levels remain high relative to the global average, this trend is concerning, as it may signal perceived gaps in transparency or integrity of enforcement, especially with respect to federal procurement oversight and ethics watchdog. After all, from a blockchain governance perspective, this level of erosion has strong justification and opportunity: that is, blockchain’s perpetual record-keeping and decentralized validation might be perceived as institutional firewall against creeping opacity.

Meanwhile, Regulatory Quality, is somewhat stable within a narrower band, improving slightly after a drop in 2020 but not coming back to previous peaks. This reinforces the perception that Canada is a very competent regulatory state, still with some bumps in the road of innovation, even some things appear relatively stable and may seem historical multiple levels above some crisis some government officials may experience when addressing autonomous digital tech.

The very slight recovery in 2022–2023 corresponds to an apparent revitalization of a federal-level national digital policy alignment about the components of this portfolio – i.e. open government, procurement modernization, interoperability standards, all foundational building-blocks for a blockchain.

With a slight downturn being perhaps the most severe development of the past eight years, the drop in Rule of Law from 1.81 (2015) to 1.47 (2023) is concerning for longer-term legal certainty. There are multiple reasons for this trend, including a relatively slow adaptation of legal frameworks to digital technologies, varying degrees of access to administrative justice, or complex and evolving challenges to align provincial and federal authority in tech-related spheres. All of which are meaningful obstacles to institutionalizing blockchain as an down-stream anti-corruption initiative, especially as implementing smart contracts, tokenized assets, and cryptographic records will call for legal validation and legitimacy (in court). Well, of course, even a tolerable rule of law environment can pose challenges

In conclusion, the figure tells us that while the governance environment is unlikely to get worse and is still very favorable for blockchain-enabled procurement reform, there are still vulnerabilities apparent from visualized trajectory. The visualized changes in governance levels suggest that Canada's success in implementing blockchain solutions will be more dependent on renewing the desire to regulate, administer effectively, and respond legally to emerging digital norms than any readiness to use blockchain technology.

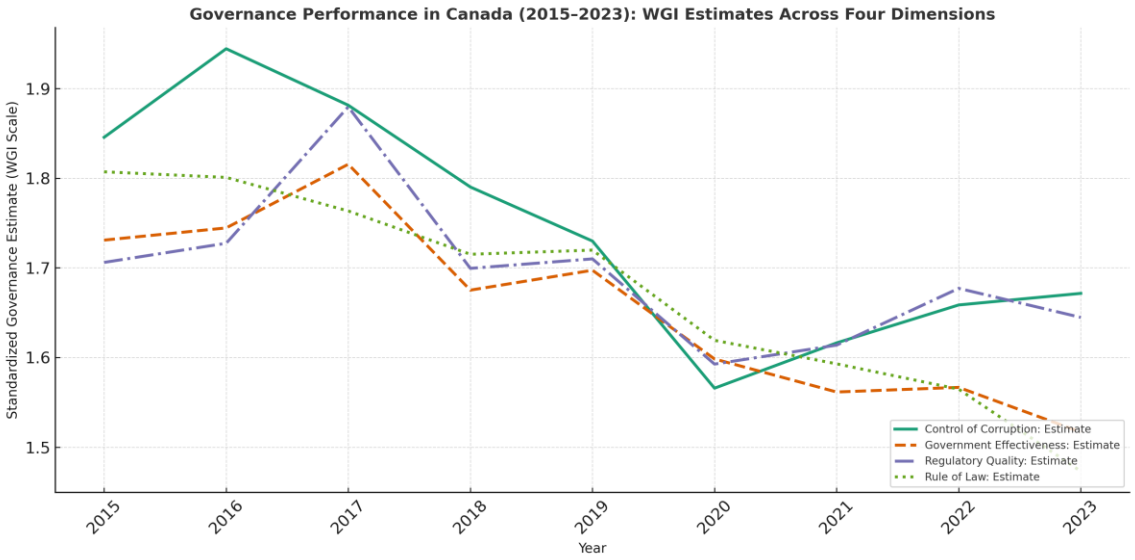

Figure 5. Canada's Governance Trajectory (2015–2023): Control of Corruption, Effectiveness, Regulatory Quality, and Rule of Law

Governance Trends in the United States: Accountability, Implications for Blockchain-Based Procurement Reform, and Institutional Variability from 2015 to 2023.

The U.S. represents an unprecedented institutional profile among high-capacity democracies, as it has pulsated between strong formal governance but also observed volatility in several governance

dimensions in recent years. Utilizing standardized estimates from the World Bank's Worldwide Governance Indicators (WGI), this analysis will explore the 'U.S. trajectory in the four pillars: Control of Corruption, Government Effectiveness, Regulatory Quality, and Rule of Law' for the years between 2015 and 2023. These scores serve as diagnostic indicators of systemic resilience, as well as drivers of receptivity to public sector innovations, such as, for example, blockchain-based procurement reform. Although the U.S. is ranked higher than most countries in the world rankings, there has been a noticeable drop in a number, but not all, dimensions after 2018, which raises questions about the temporal consistency of institutional performance in a more complex political context.

The Control of Corruption score for the U.S. started with an estimated value of 1.36 in 2015 that peaked at 1.34 in 2017, before entering a distinct downward spiral to 1.04 in 2020 and escalating slightly to 1.12 in 2023. One can observe the downward trajectory corresponds with the heightened scrutiny regarding political patronage, opaque campaign finance operations, and conflict-of-interest at both federal and state governance mechanisms. As this path changes thinking about blockchain-based procurement reform, it has a dual-state condition: it is on one hand uncovering systemic weaknesses that blockchain might be able to mitigate—especially in terms of improving traceability and eliminating discretionary power in contracting allocation. Meanwhile, with decreasing control of corruption, it can also suggest that institutions may not welcome this type of transparency-enhancing tools, if the tools are viewed as a threat by powerful actors to their existing discretionary practices. In the specific context of the U.S., the value of blockchain may lie more in ensuring that automated, auditable procurement transactions are delivered on the local sub-federal level, where the highest variability of institutional integrity exists.

Government Effectiveness—one of the critical dimensions of digital transformation—declined from 1.43 in 2015, gradually increased to 1.54 in 2018, and fell to 1.22 in 2023. This downward trend of approximately .20 points in effectiveness courts a variety of challenges related to political polarization, agency turnover, and policy inconsistency that removes the aggregate capacity of implementation among federal agencies. To be clear, declines in effectiveness do not suggest a lack of state capacity but a decay of the state's internal coherence and foresight. This lack of cohesion is particularly important with regard to the increased use of digital technologies for public purposes such as blockchain, which require partnership, sustained budgets, and long-term alignment of governance across implementing agencies. As opposed to a fully centralized approach to procurement as is retained federally, the decentralized nature of U.S. procurement results in thousands of actors that all come with their respective standards, business partners, and legal regimes. Thus, it is increasingly complicated to effectuate change—both in terms of diffusion and institutionalization, the separation of the public procurement dimension and efforts to include blockchain as a supporting technology. If these reforms are to be effective, strategic opening of policy windows is important to create (or couple to forms of central digital investment such as national cybersecurity frameworks or infrastructure modernization initiatives).

Regulatory quality is a representation of one of the most dynamic trajectories of the four dimensions. Beginning with a score of 1.24 in 2015, regulatory quality drastically increased to 1.62 in 2017 with an influx of deregulatory initiatives and business-friendly reforms. However, since it reached a local peak at 1.62, there was a plunge to 1.24 in 2020, followed by an increase to 1.44 in a volatile 2021, then another drop back to 1.39 in 2023. The oscillations of this indicator demonstrate that the political and administrative contestation of regulatory quality has persisted in the U.S.—especially against regulatory adjustments on issues of digital governance, data privacy, and federal procurement modernization. From a blockchain integration perspective, regulatory quality is an essential enabler for the true nationalization of barriers comprising 1.) the creation of pathways for legal and economic innovation, and 2.) the provision of reliable standards for interoperability to link systems of governance (across levels of government) in the process of blockchain insertion. The volatility of this transaction shows how fragmented, fragmented and reportedly politicized regulatory policymaking can remain in the U.S. even though there is a vision to retool through the insertion of blockchain unless processes are backed by mandates from the Federal Directorate or include broad consensus model legislation. The change in the Rule of Law indicator value, from 1.56 in 2015 to a high of 1.61 in 2017 to a diminishing value of 1.33 in 2023, reveals weak but disparate processes that point to rising concerns of judicial independence, asymmetrical enforcement and access to remedy (notably during politically charged procurement scenarios in procurement disputes, or access to administrative appeals). The above is important to articulate for blockchain reforms, as legal enforceability of smart contracts, recognition of cryptographic evidence, and other dispute mechanisms requires clear articulation and consistent application. The overall decline will probably not compromise blockchain adoption or preclude scaling, while underscoring that legal modernization must happen simultaneously. Without simultaneous modernization, blockchain potentially could be operationally functional without being operationally unclear, as some jurisdictions have not undertaken an update to their respective procurement laws in tandem with development of technology.

Taken collectively, the U.S. governance indicators for 2015 to 2023 depict a system with established institutional capacities, but increasing internal fragmentation and differences. This has significant implications for the design and deployment of new blockchain based procurement platforms. In weaker governance environments, blockchain is generally envisioned as an alternative to the existing mechanisms. In the case of the U.S., the technology will more closely reinforce adherence to implicit/explicit laws, automate compliance checks and strict oversight, and bridge coordination failures across agencies. The distribution on these outcomes will primarily depend on the order of technological implementation, as well as harmonization of procurement codes across jurisdictions, as well as building legal regimes that formally recognize and adjudicate digital instruments. Thus, the U.S. represents both a great developmental opportunity and a challenge of institutional complexity for blockchain-enabled anti-corruption innovation - a careful balance between technological ambition and institutional realism is needed.

Table 9.Table 3.5.4.4.4. U.S. Institutional Performance Across Four WGI Dimensions, 2015–2023

Year	Control of Corruption: Estimate	Government Effectiveness: Estimate	Regulatory Quality: Estimate	Rule of Law: Estimate
2015	1.358	1.432	1.242	1.563
2016	1.331	1.441	1.486	1.581
2017	1.341	1.517	1.619	1.609
2018	1.293	1.537	1.613	1.476
2019	1.180	1.453	1.335	1.424
2020	1.038	1.275	1.238	1.336
2021	1.019	1.298	1.441	1.389
2022	1.104	1.255	1.424	1.369
2023	1.123	1.217	1.394	1.328

Note. Data from World Bank (2023). Worldwide Governance Indicators. Standardized governance estimates range from −2.5 (weak) to +2.5 (strong).

Figure 6.3. Governance Performance in the United States (2015-2023): Longitudinal Trends in Institutional Capacity Based on World Bank WGI Indicators.

This figure portrays a longitudinal analysis of the United States' institutional governance across four standardized dimensions Appeal WGI-World Governance Indicators - Control of Corruption, Government Effectiveness, Regulatory Quality, and Rule of Law - from 2015 through 2023. The data shown is from the WGI, which essentially estimates government at the country level by means of a normalized scale allowing cross-temporal comparisons across the four dimensions critical in assessing the suitability of blockchain-based reforms in public procurement. The four dimensions are detailed, illustrating the US continues to command high rankings, particularly relative to other countries but the period after 2017 evidences moderated declines across all indicators which, a reality in the context of ingrained institutional volatility and fragmentation in US policy.

Of the four dimensions, the controls of corruption dimension have a more consistent decline, a decline from 1.36 in 2015 to 1.12 in 2023 - with the sharpest decline from 2018 to 2020. While the rating remains well above the average and noticeably high relative to other countries, the decline reflects increasing concerns with opaque sources of influence in government-led areas, political accountability, and inconsistent enforcement of integrity norms, which have direct

implications for procurement trust. From a blockchain-instrumented governance perspective this offers both a requirement for adoption and a chore: on one hand, distributed ledger technology allows audits of transactions, limits discretion in process - in other words it is meaningful in some regard, but in an environment with fluctuating scores, stakeholder alignment is critical to maintaining and enhancing the probability of legal legitimacy and integrity.

Government Effectiveness trend similarly, albeit starting at 1.43 in 2015, peaking at 1.54 in 2018, and demonstrating a decline to 1.22 by 2023. In this time frame it reflects perceived declines in the nature and quality of public administration, identified delays in policy implementation, and higher degree of turnover in government performance. If the trajectory doesn't change, it is difficult to believe that institutionalization will happen with blockchain tools. A sustained stream of benefit accruement does not happen simply by technical deployment of technology; it requires continuous buy-in from relevant administrative leaders, interoperability standards, and performance monitoring. Therefore, a public administration without a demonstrated capacity for consistently high performance will continue to lead to fragmentation of blockchain performance.

Regulatory Quality and Rule of Law has demonstrated a greater degree of volatility which is a factor of larger legal and policy uncertainty - Regulatory Quality increased quickly to 1.62 in 2017, declining to 1.24 in 2020, and then gradually increased to 1.39 in 2023. Meaning this is characterized by regulatory oscillation which can only be described as declining confidence for regulatory certainty, at times, emerging from variances in federal policy direction and sub-federal uncertainty. If the systematic implementation of a series of blockchain assets is contingent on an adaptive and innovation-friendly regulatory environment, i.e. procurement codes, smart contract legal validation, digital contracts with a legal signature, this is likely going to be a hard contribution outside capitalizing for blockchain benefits. Finally, Rule of Law (which peaked at 1.61 in 2017) has fallen to 1.33 in 2023. It seems there are issues with faith in legal certainty, equality in enforcement, and trust in institutions. For blockchain to demonstrate its potential to automate enforcement and establish immutable ledgers it must be supported with these building blocks. If legal contexts are perceived as rife with unpredictability or fragmentation, the repudiation of the interpretability and enforceability of Smart Contracts becomes debatable. Thus, legal modernization needs to accompany the deployment of technology so it can avoid systemic dissonance.

Thus, overall, the figure shows a governance profile that is weak, on the whole, but globally accepted. Notably, though, we see evidence of institutional drift and weaknesses across several critical dimensions. If the U.S. is to take advantage of blockchain´s promise in the reform of procurement, the observed decline illustrates the process of re-strengthening administrative effectiveness, sustainable regulations, and legal regime. The demonstration data helps support a policy posture that shows blockchain not as a bullet but as part of a realization of a broader institutional revitalization and digitization transparency strategy.

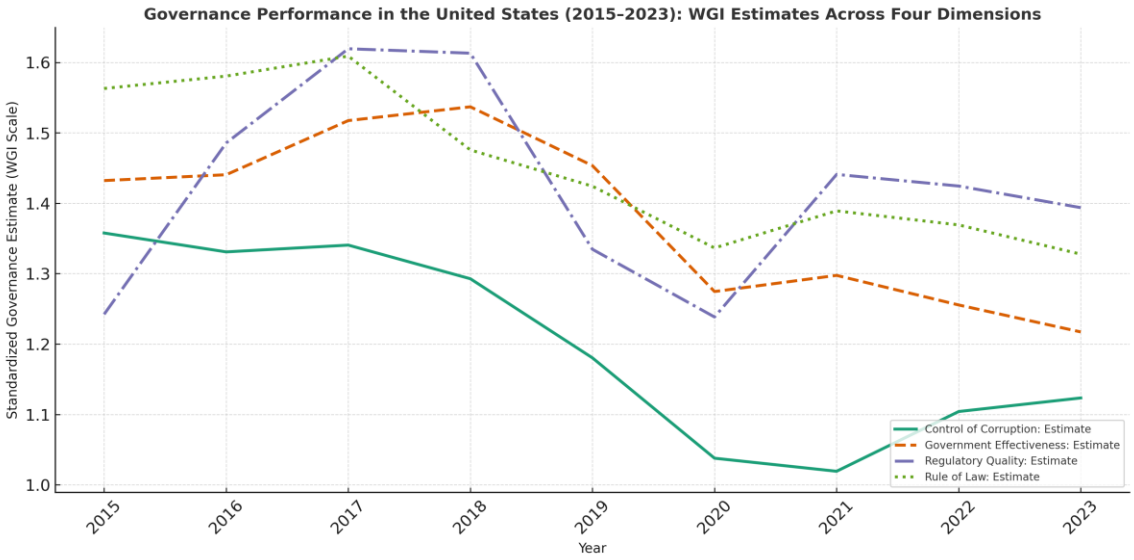

Figure 6.Figure U.S. Institutional Capacity Over Time (2015–2023) Based on World Bank Governance Estimates

Cross-Country Contextual Dynamics (2015-2023): Governing Institutions to Facilitate Blockchain-Reform Procurement Radical Innovations

The cross-national development of governance indicators in Italy, Canada, and the United States over the 2015-2023 period, provides important empirical context and assessment regarding the opportunity for blockchain adoption in public procurement. Based on the global governance analysis framework of the Worldwide Governance Indicators (WGI), the present project will profile the comparative development of four interdependent governance dimensions, including: Control of Corruption (CC), Government Effectiveness (GE), Regulatory Quality (RQ), and the Rule of Law (RL). These governance indicators are proxies for institutional integrity, organizational capacity, operational nimbleness, and legal certainty, respectively. Importantly, the four interdependent governance dimensions - CC, GE, RQ, and RL- establish the key governing conditions or pre-conditions on whether digital, distributed ledger technologies can integrate into procurement systems using governance principles. The longitudinal pathways of governance across the three jurisdictions demonstrate points of connection and distances in the institutional readiness for digital anti-corruption governance solutions.

Control of Corruption presents the clearest difference is governance pathways. The sector improvements observed in Italy is notable, as CC scores were 0.03 in 2015, and improved to 0.55 in 2023. This significant improvement suggests successful domestic reforms, and enhanced

convergence between national reform efforts and evolving EU procurement reforms designed to enhance procurement transparency through digital enforcement. The pathway suggests a progressive governance position to control discretionary abuse through system-wide institutional reform, establishing a significant opportunity for blockchain longevity associated technologies to offer immutable and transparent recordkeeping. In contrast, Canada – informed by its initial integrity advantage - results in a subtle but consistent decline from a peak of 1.94 in 2016 to 1.67 in 2023. These scores remain within the global high-band for performance, however each year has established a descending slope in public trust for elite accountability and ethics oversight, warranting another exploration in new anti-trust enforcement technologies, such as blockchain. The United States shows the greatest instability with scores dropping from 1.36 to 1.12 - witnessed as institutional fragility with regards to political ethics structuring, lobbying behavior, and regulatory enforcement asymmetries. In the U.S. context, the interaction of blockchain may be less about institutional enforcement governing principles, and more about standing-in for fragmentation, and enabling auditability emergent from non-federal governance systems were. or improve various degrees within their public procurement integrity.

These findings reveal an important premise regarding the probability of blockchain incrimination in procurement reform. In situ jurisdictions such as Italy that have shown improvement in controlling corruption, may be relatively more receptive to blockchain technology as an adjunct to ongoing reforms. Canada and the United States - despite their relative high positions in integrity - possess more of an institutional disconnect if their governance perception of blockchain as a potential external interruption (disruption) for their administration, rather than complementary administrative tool. Thus, new anti-corruption blockchain initiatives must be tuned or aware of the political economy of institutional change, and corresponds to the governance maturity that either jurisdiction currently occupies.

Comparative Administrative Capacity and Blockchain Feasibility: Government Effectiveness as a Constraint and Enabler

The Government Effectiveness indicator assesses public sector perceptions about the quality of public services, the independence and professionalism of civil service, and credibility of government commitments to sound policies. Each of these attributes is an essential condition for implementing blockchain in public procurement. Verifying a state’s ability to adopt blockchain technologies is not merely dependent upon basic infrastructure and funding, but also the state’s constant ability to integrate, implement sustainable policies, and institutional adaptability. The Government Effectiveness data for Italy, Canada, and the US between 2015-2023 illustrate substantial differences in trajectories of administrative performance that affect how effectively and sustainably a jurisdiction can achieve blockchain-enabled reform.

Italy's Government Effectiveness score fluctuated considerably during the reference period. From 0.49 in 2015, Italy’s Government Effectiveness score peaked at 0.54 in 2016, before falling to 0.36 by 2020, and recovering after 2020 to peak 0.61 in 2023 - the highest score in the entire observation

period. This confluence of peaks and troughs indicates a structural instability in Italy's public administration characterized by political discontinuities with so much fragmentation of institutionally-defined responsibilities that the public administration cannot sustain the continuity of improvement in its capabilities. The rebound post-2020 is naturally correlated with the European Union Recovery and Resilience Facility (RRF) which provided member states incentives to put their digital services on the digital service agenda, improve public procurement transparency, and modernize their administrative activities. Although the investment has ostensibly enhanced their digital readiness, the years preceding it highlighted the damage that years (over a decade) of administrative interruption can cause when tipping towards an over-dependency on technology adoption without any parallel improvements to the bureaucratic capacity, policy coordination, and accountability structures of the organization. For the state of Italy, when contemplating blockchain adoption, the idea of exploring it must align to its implementation governance in order for it to not become an ornamental/figurative reform example that fails to then develop operationally.

In contrast, Canada started from a higher base, with a Government Effectiveness score of 1.73 in 2015, peaking at 1.82 in 2017, before declining to 1.52 by 2023. Although this score indicates that Canada's public sector remains a globally high performer, this data trajectory indicates a reduced agility, and an increased friction to effective policy co-ordination, particularly across federal and provincial jurisdictions. The period post-2020 reflects the pressures of the logistics of pandemic response within overlapping digital systems and the limited systematic coherence of long-term innovation strategies. From the perspective of failing to achieve successful institutionalization of blockchain systems within Canada's procurement systems, greater policy coherence and intergovernmental alignment in new public management is required, or alternative decentralized technological solutions will become the catalyst for additional fragmentation caused by previous public-sector incoherence. In the U.S., Government Effectiveness has a similar awning to Canada to avoid becoming a geographic troll but with sharper reductions. It increased from 1.43 in 2015, to 1.54 to 2018, and fell to 1.22 in 2023 - reflective of the chronic dysfunction of bureaucratic continuity, particularly when considering polarized political transitions, unreliable budgeting essential planning, and an entitlement to bureaucracy. This has created a dilemma. The U.S. has extensive technology and human capital, yet its ability to actualize the bureaucracy of blockchain complex reforms is hampered by a disconnect in institutional turnover and drop-off of executive priorities. Centralized coordination and extended digital planning will be central; absent these contextual conditions, blockchain-aided transactions will only be implemented as pilot projects and state-level implementations with varying adaptability and limit scale in interoperability and evaluability.

When taken together, these findings reveal that government effectiveness represents a necessary but not sufficient condition for success to be realized in blockchain ecosystems. The gains made by Italy this proliferation cycle are certainly encouraging and demonstrate that external conditionalities (e.g. E.U. Funding) can provide leverage to support reform but, the zeitgeist of internal administrative reform must precede sustained advances. Similarly to Canada, the U.S.

demonstrated considerable capability, but indications are toward virtualization being a catch-up campaign with systemic drift underscoring made-for-sustaining institutional recommitment to undertake coordinated innovations in public sector innovation. Other than waiting for the market-driven conditions to result in coalesce new suppliers, the available inkling of compatibility of administrative capacity with country blockchain deployment will be important not only for adoption, but for reasonably provisioned, auditable, and interoperable digital experiences within public procurement ecosystems.

Regulatory Quality and Legal Pre-Wayne: Comparative Normative Environments for Blockchain Governance

Regulatory Quality refers to perceptions of a government's ability to formulate and implement sound policies and regulations that permit and provide opportunities for private sector development. For blockchain-based procurement reforms, this specific indicator is fundamental as it reflects the degree of coherence, adaptability, and forward-compatibility of the legal-regulatory climate in which blockchain architectures must operate. Smart-compliant contracts, distributed databases, cryptographic identities all require enabling regulation to legally and operationally function with public institutions. The governmental pathways of Italy, Canada and the U.S. provide examples of the promise and peril of proceeding with blockchain proposals.

Italy's regulatory quality rankings generally vary significantly, rising from 0.71 in 2015, soaring to a mid-cycle peak of 0.94 in 2019; however, from 2019 onwards, Italy exhibited rapid decline falling to 0.49 in 2020, and recovering marginally to 0.67 in the last report (2023). Italy's peak in 2019 mirrored an ambitious spin of digital policy experimentation, including initial extensions of e-procurement platforms, regulatory sandboxes, and the introduction of the Public Digital Identity System (SPID). Yearber the post-pandemic period of restorative regulations that may engage to bolster evidence-based governance. Italy's subsequent drop off with the COVID-19 experience illustrated the susceptibility for the disruptions of authorities incurred through emergency disasters in policy enforcement to reduce the implementation of creative governance practices. Not establishing an operational equilibrium by 2023, suggest an active engagement of expectations and potential of hallmarks of administrative stability. For blockchain to establish continuity in Italy, regulatory observants need not only stabilize but also anticipate the possibility of regulatory infrastructures that anticipate governance of emerging technologies without relying on excessive case-by-case exceptions. Canada exhibits a more stable, but modestly downward trend. While it peaked at 1.88 in 2017, by 2023, Canada's regulatory quality declines to 1.64, with the nadir at 1.59 in 2020—which, once again, coincides with a peak of "emergency governance." Although the decline is less pronounced than with Italy, it is still serious. Canada has, traditionally, been recognized for the predictability, inclusivity, and responsiveness of its regulatory institutions. However, this data suggests that regulatory innovation has at least not kept pace with technological change, particularly in the form of digital procurement standards, the legality of blockchain, or AI-enabled adjudication optimizations in contract oversight. To avoid regulatory stasis, Canadian authorities should not only recalibrate frameworks to accommodate blockchain, but to facilitate

blockchain integration by, for example, specifying the legal status of smart contracts, standardizing the audit of cryptographic protocols, and by regulating the governance of data in federal procurement-specific platforms.

The United States displays a more erratic pattern, climbing from 1.24 in 2015 (federal regulations promulgated) to 1.62 in 2017 (deregulatory enthusiasm) before returning to 1.24 in 2020 (social unrest) only to partially rebound to 1.39 in 2023 (federalization). These fluctuations signal the highly politicized nature of U.S. regulatory policymaking and its downstream authority fragmentation among federal and state jurisdictions. The episodic nature of exuberance surrounding deregulatory action artificially inflates regulatory quality metrics, but the long-term effects can result in a fragmented regulatory trade environment, legal uncertainty, and, reversals of policy. This instability creates risk of great significance for blockchain deployment. In the absence of consistent federal guidance or unified procurement law between states, blockchain solutions may be plagued with legal uncertainty, poor interoperability, or untenable opposition. Innovation may also struggle if the agency lacks jurisdiction or if face two levels of compliance obligations (at both state and federal level).

In comparative context, while Italy's fluctuations, Canada has shown gradual decline and the U.S. has entrenched fragmentation, each arguably presents unique regulatory challenges for blockchain-enabled procurement. Regulatory quality is not simply an indicator and/or facilitator of innovation, it is a guarantee of legal predictability—especially in public contracting situations with automated logic, immutable audits, and digital identities. Moving forward, all three jurisdictions will likely have to strengthen their regulatory institutions—this does not mean having more regulatory regimes, but better, more robust, and fit-for-purpose governance frameworks that respect and accommodate the tension between legal formality and technological fluidity. Rule of Law & Blockchain Feasibility: Legal Preconditions for Digital Integrity in Public Procurement

Among the four governance dimensions discussed in Italy, Canada, and the USA, the most legally determining dimension to potentially succeed, legitimize, and scale blockchain-based anti-corruption work in public procurement is Rule of Law. In this dimension, we account for (1) the extent of institutional trust toward a legal environment, (2) the extent for predictability in the enforcement of a contract (if there is one), and (3) whether the judicial process can offer administrative justice—all of which serve as foundational elements toward facilitating opportunities for smart contracts and distributed ledgers in the public procurement ecosystem. The trends you identified with Rule of Law across the three countries—weigh equally against the differences in institutional capacity to absorb the systemic digital transformation, legally—in making a point that the scalars regarding blockchain-based anti-corruption potential in procurement is inevitably predicated on (1) the digital capacity in existence, not only its full spectrum of digital capacity; and importantly (2) the flexibility of the legal environment/system.

Italy's Rule of Law values range between 0.21 and 0.39 from 2015 to 2023, illustrating the continuing legal fragility involved in enforcing even a blockchain-based public procurement

system, which presents enormous challenges. These values highlight issues—judicial efficiency, administrative delays, and levels of legal clarity—particularly regarding monitoring contract disputes, or parties engaged in the public tender process. In the case of Italy, findings reported in chapter six, suggest an institutional capacity for digital transformation to public procurement by precedence, even providing mandates or reforms (e.g., ANAC or EU) was greater than the courts capacity to cognize or imagine, during their decisions, there was an equivalency to blockchain and automated contracts. This disordered disjunction between the technical ambition of blockchain and legal institutional infrastructure is an unexamined gap in the literature, that presumes too much in regard to digital governance initiatives, rests within intentionally constructed rule-of-law environments. The study in Italy was illuminating in exposing the legal infrastructure barrier, and reinforces my original contribution to the dissertation, novel thought about how to conceptualize minimum thresholds of legally enforceable agreements as a precondition of institutionalization for blockchain delivery in public procurement.

Although Canada has comparatively greater values of Rule of Law—averaging 1.81 in 2015, and 1.47 in 2023—it is an equally treacherous case as a reflection of an increasingly legal fragmented federated society. While the legal environment, and the legal capacity remain outside of serious peril, there is an unmistakable decline in "the confidence that the law is applied uniformly and equally to all the individuals and groups in society"—and especially after 2019, this is concerning regarding increased complexity when adjudicating new digital governance instruments. In our public procurement context, this is troubling in terms of harmonizing blockchain friendly reforms around both federal/provincial jurisdictional concerns, especially along offence taking smart contracts, surrounded by context-dependent procurement codes. The dissertation therefore fills a void in the social scientific literature, modelling how the historical realities of intergovernmental legal structures may in fact obstruct learning through ambiguity; or even create an additional layer of complexity, which may inhibit the scalability of blockchain, even though it will be built upon a significant institutional baseline. In this vein, the dissertation supports one theoretical assumption: that legal centralization as a principle may have greater consequence as a premise than its legitimate strength; as a lawful centralization may be a better predictor of the ultimate readiness of legal environments to direct blockchain adoption and use, particularly when embedded within federated environments.

The United States shows the most complex trajectory pattern of Rule of Law, declining from 1.56 in 2015 to 1.33 in 2023 despite being the world leader in legal and technological infrastructure. This paradox plays into one of the major research questions for this dissertation: To what extent can high-capacity systems with fragmented legal authority institutionalize blockchain in a manner that is both operationally and legally coherent? The U.S. case study illustrates that in even high innovation capacity contexts, the lack of harmonized legal regimes for blockchain procurement law at the federal, state, and municipal levels creates significant uncertainty concerning smart contracts recognition, admitting cryptographic evidence, and digital dispute resolution. The study includes a new compliance-alignment table that cross-references variability of jurisdictional

procurement law against the procedural logic of blockchain-- providing a directional tool for determining the legal readiness and comparing the levels of legal readiness across multilayer forms of governance.

In conclusion, Rule of Law appears as necessary legal backbone for blockchain enabled reform in procurement-- but it is an inconsistent and differently behaving legal backbone in Italy, Canada and the United States. Italy experiences systemic fragility, Canada experiences jurisdictional fragmentation and the United States experiences the legality of legal pluralism and ambition for digital governance capabilities. The author’s conclusions support the dissertation's assertions that blockchain law is not grounded in technological determinism or institutional neutrality but is completely contingent on whether digital innovation and the normative architecture of public law are aligned at deep structural level. By integrating genealogical governance analysis with comparative law-regulatory field, this study provides an original and mechanism-based contribution to the new field of blockchain public administration-- filling an identifiable gap in both the literature on blockchain or both attitudes towards current public procurement reform.

The comparative analysis of the trajectory of governance in procurement in Italy, Canada and the United States between 2015-2023 provides very specific policy insights on the use of blockchain-based anti-corruption reform in public procurement. While Canada and the United States exhibited very high institutional baselines as jurisdictions, results indicate both have scored declines in key measures of government effectiveness and the rule of law indicating that consistent administrative and legal convergence with blockchain may be in obstacles for future performance. Italy too is making progress on controlling corruption and effectiveness dimensions but is limited by its enduring structural weaknesses in legal enforceability and regulatory stability. These patterns demonstrate that feasibility issues related to blockchain are influenced less by static governance capacity issues than dynamic distinct institutional convergence variables. This leads to the recommendation that a blockchain-based solution needs to be pursued not as homogeneous but as a sequenced policy prescription approach: in Italy, large-scale adoption of blockchain may need to be preceded by legal modernization, and the clarification of the judicial process; in Canada, policy upgrade through intergovernmental legal harmonization is, if not a prerequisite, critical; and in the United States, coherent and unified regulation that support interconnectional harmonization are essential to uphold. This repetition reinforces the key claim of the dissertation original claim is that blockchain can be successful in public procurement but will depend on specific levels of technical maturity as well as aligned reform across legal, regulatory and institutional supports.

Table 10.Table 3.5.4.5.6 Governance Indicator Trends by Country and Year (2015–2023): A Foundation for Blockchain Feasibility Assessment

Country	Year	Control of Corruption	Government Effectiveness	Regulatory Quality	Rule of Law
Italy	2015	0.03	0.49	0.71	0.29
Italy	2023	0.55	0.61	0.64	0.39
Canada	2015	1.85	1.73	1.71	1.81
Canada	2023	1.67	1.52	1.65	1.47
United States	2015	1.36	1.43	1.24	1.56
United States	2023	1.12	1.22	1.39	1.33

The table above summarizes the performance of Italy, Canada, and the United States on the four important WGI dimensions of digital integrity and the use of blockchain in public procurement. The presentation of both the baseline (2015) and recent (2023) scores allows for cross-country benchmarking of institutional pathways over the last ten years. These indicators act as an evidence-based proxies for the evaluative framework of the dissertation that examines the feasibility of blockchain as an anti-corruption tool in the context of public contracting shaped by legal, regulatory, and administrative factors.

Source: Author's compilation using data from the World Bank's Worldwide Governance Indicators (2023).

The comparison of standardized worldwide governance indicator (WGI) scores for Italy, Canada, and the United States is depicted in this heatmap. The four dimensions of governance that were used for the comparative heatmaps are Control of Corruption, Government Effectiveness, Regulatory Quality, and Rule of Law at two points in time, 2015 and 2023. This heatmap helps users to longitudinally assess the institutional readiness to adopt blockchain-enabled anti-corruption reform in public procurement. The temporal and jurisdictional divergences captured in the figure reveal pertinent differences in legal enforceability, administrative capacity, and regulatory coherence, each fundamental conditions for positive deployment of distributed ledger technologies in complex procurement environments.

Source: Author’s visualization based on World Bank WGI data (2023).

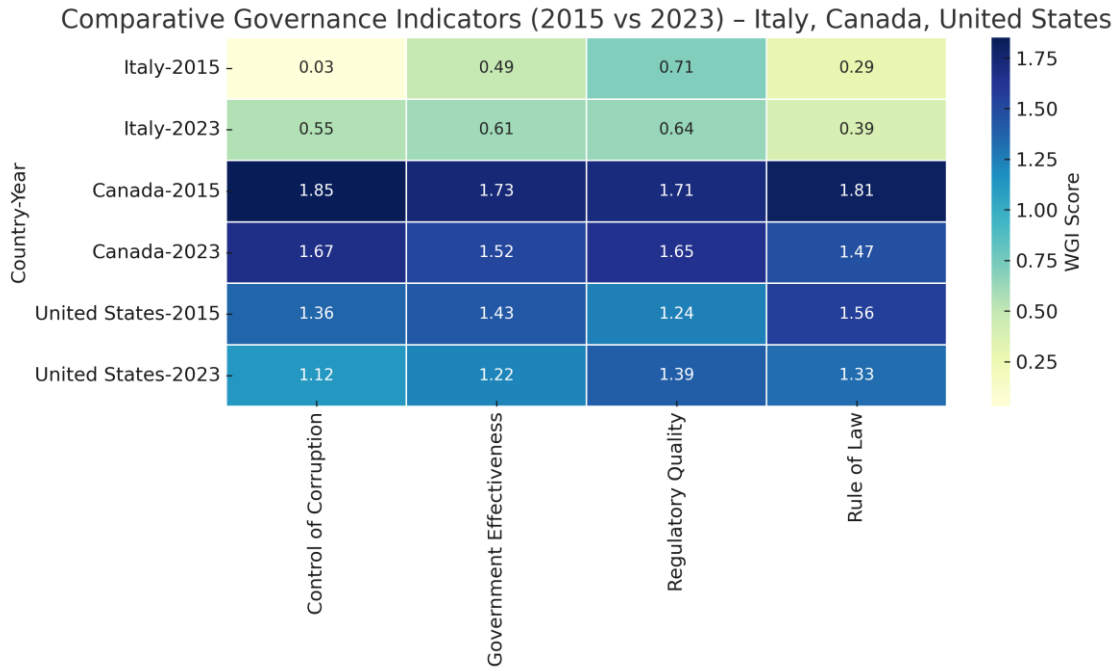

Figure 7.Comparative Heatmap of Governance Quality (2015 vs 2023): Italy, Canada, and the United States

3.6. Comparative Regulatory Frameworks for Blockchain in Public Procurement

3.6.1. Italy's Regulatory Approaches (EU context)

Italy takes a technology-neutral, legally enabling regulatory approach to blockchain in public procurement, making institutional roles and legally enforceable obligations regarding data governance clear. The Autorità Nazionale Anticorruzione (ANAC) regulates the procurement backbone of data, and legal publicity via the Banca Dati Nazionale dei Contratti Pubblici (BDNCP) which ANAC runs in conjunction with a series of binding acts (Delibera n. 261/2023 information flows to the BDNCP (implementing art. 23 of the new Code), Delibera n. 262/2023 Fascicolo Virtuale dell'Operatore Economico (FVOE), Delibera n. 263/2023 legal publicity and Delibera n. 264/2023 transparency; ANAC, 2023a, 2023b, 2023c, 2023d). The AgID (Agenzia per l'Italia Digitale) national digital plan indicates the minimum technical and interoperability features for the BDNCP (AgID, 2024). In fact, the plan indicates that with respect to interoperability of certified procurement platforms to national and EU services there is no need for one-off adapters (AgID, 2024). This cluster of authorities and responsibilities sit interlaced with the Public Contracts Code (Legislative Decree No. 36/2023) which prescribes end-end electronic processes, machine-readable transparency over the lifecycle of contracts; enforceable on an EU requirement to use secure electronic communications and structured standardized notifications; Directive

2014/24/EU, art. 22 and Regulation (EU) 2019/1780. The net result is a procurement ecosystem that is an obligation under the law to be 'digital by default' with traceability, time-sequencing and auditability as compliance obligations that fit into previously specified policy choices (ANAC, 2023a-d; AgID, 2024; Legislative Decree No. 36/2023).

With this context established Italy has also created the general civil-law hook for distributed ledgers, but one things seems very clear from our analysis of how} Italian regulators are thinking about the possibilities of blockchain for public procurement, they are starting from the end-to-end procurement digitalization experiences and processes which fed into the Digital Gov12/2019, is an artifact that defines decentralized networks and distributed architecture, innovates on "smart contracts" conceptually, recognizes legal impacts (meaning conditionally equivalently written), and conceives irreversible and time-stamped, and verifiable actions readily recognizable in an administrative capacity (Decree-Law No. 135/2018, art. 8-ter). Across the context of procurement workflows, there are no binding ANAC or AgID sector-specific guidelines that operationalize DLT, meaning that current values are DLT contextually compatible while concurrently allowing for technology-neutral values. Policymaking instruments have provided engendered and manageable routes to operationalize that level: domestically through the FinTech Regulatory Sandbox (Ministerial Decree No. 100/2021), which permits supervised experimentation within a time-constraint and iterative governance structure, which is recyclable for permissioned DLT pilots within public travel; at the supra-national level, the DLT Pilot Regime specifies supervision for ledger-based market infrastructures; whilst the recast eIDAS will establish European Digital Identity Wallets and verifiable notifications of traits; which will be the rails for procurement platform onboarding suppliers and considering eligibility decisions within FVOE (Regulation (EU) 2022/858; Regulation (EU) 2024/1183).

The main challenges relate to legal-technical and institutional. GDPR rights of rectification and erasure are in structural contradiction with the permanence inherent in immutable on-chain capabilities, preferable in hybrid arrangements where personal and commercially sensitive data remains off-chain with proof or hashes registered on-chain (Regulation (EU) 2016/679). Cybersecurity obligations are agnostic – the existence of a National Cybersecurity Agency, the follow-up on government cloud posture, and assessing the protection of critical databases impose a level of risk-classification and access-control, and incident reporting (Decree-Law No. 82/2021; ACN, 2024a, 2024b).Market structure compounds those frictions: a concentrated ecosystem of e-procurement vendors in concert with a failure to face technical annexes that take DLT as a given can give rise to path dependence (high switching costs and proprietary schemas), a type of “soft” capture that invites authorities to optimize for short-term BDNCP/eForms regulatory compliance over long-term verifiable-credential or tamper-evident innovations. Still, the possibilities are tangible and pressing: evidentiary integrity in submissions and exchanges through permissioned-ledger proofs reconciled with BDNCP clearances; supplier due-diligence through eIDAS-conformant attestations linking to FVOE; and tamper-evident change-order and milestone trails that strengthen ex post accountability without delegating discretionary judgments (ANAC, 2023a–

d; Regulation (EU) 2024/1183). Conclusion: Italy—entrenched EU-based procurement regime—has amassed the normative and technical building blocks for lawful, privative, and cyber secure blockchain uptake: ANAC binding data-governance acts; AgID interoperable standards; civil-law consent for DLT/smart contracts; and identity/credential rails. What's missing is the concentrated activation. A co-ANAC and AgID guideline should concretize permissioned-DLT patterns (off-chain personal data; on-chain proofs; wallet/attestation verification for FVOE), confirm the evidentiary status and retention of ledger events within administrative procedure, and reconcile node governance and smart-contract assurances with national cybersecurity baselines. Otherwise, bureaucratic inertia and vendor lock-in will continue to stifle experimentation; with it, Italy can turn technology-neutral lawfulness into verifiable reputable practice competitive and resistant to corruption.

3.6.2. Regulatory Approaches in Canada

Canada's pathway to blockchain in public procurement is straitjacketed through federalism. The procurement and digital governance processes are shared responsibilities across federal and provincial orders of government with specific federal policy (e.g., service-digitization, interoperability, data stewardship) existing in parallel with provincial jurisdiction over "property and civil rights" and local procurement systems. The result is a governance space that is enabling, but fragmented. While it articulates principles consistent with distributed ledgers (e.g., traceability, structured data, security of exchanges), it does not have a single authority or level of government that can obligate or certify blockchain uses inside all procurement systems (Constitution Act, 1867, s. 92).

In this system, the roles exist differentiable and functionally rather than centralized. At the federal level, horizontal digital policy and investment governance instruments (e.g., the Directive on Service and Digital; the Policy on the Planning and Management of Investments) encourage digital-by-default ways of doing business, promote interoperability, and measure auditable data flows – conditions that can technically co-exist with permissioned DLT without articulating that architecture as a requirement (TBS, 2020). Procurement operations and integrity screening are provided for through Public Services and Procurement Canada's federal procurement policy (e.g., the Ineligibility and Suspension framework) and cloud/security directives define infrastructure baselines; provinces rely entirely on their own agendas for digital trust and credentialing provision. Furthermore, Canada does not have a unitary anti-corruption regulator (e.g., Italy's ANAC); there is no level of government binding all procurement practices to one definition of legality with respect to blockchain. Rather, several authorities issue general digital rules, which are enforced on a case-by-case basis, benefiting a cautionary approach in high value tenders.

In Canada, there are no binding regulations contextualized for procurement for blockchain. Applicable law operates in an indirect manner: privacy regulations (e.g., the Privacy Act in the federal public sector, and the Personal Information Protection and Electronic Documents Act in relation to private sector providers) install accuracy and rectification duties to be reconciled against

immutability of ledgers, prompting designs towards hybrid models with off-chain personal data and on-chain proofs (Privacy Act, R.S.C. 1985, c. P-21; PIPEDA, S.C., 2000, c. 5). Algorithmic governance demands (e.g., the Directive on Automated Decision-Making) would attach in instances where smart contract logic acts present to influence eligibility, scoring, or workflow gating—such arrangements would generate impact assessments, documentation, and frameworks for human oversight (TBS, 2024). None of these instruments prohibit DLT; rather they delimit a set of compliant parameters with which a procurement-grade ledger must comply.

Policy initiatives and sandboxes represent the experimental corridor. The Canadian Securities Administrators' innovation/sandbox program (innovatively/substantively/supervised, finite-testing) has established supervised, time-framed, testing—as have many public-sector pilots in-kind. Sub-national implementations of verifiable credentials (e.g., the Verifiable Organizations Network/OrgBook lineage demonstrate implicated capabilities) illustrate, primarily, that decentralized identifiers, as well as credential proofs, which compress verification timelines for characteristics of organizations associated with vendor qualification—even if not formalized into procurement rules (Preukschat & Reed, 2021). And global standards bodies have matured the technical substrate: ISO 22739:2020 supplies a shared vocabulary for blockchain/DLT, while the W3C Verifiable Credentials Data Model specifies interoperable attestations which if mapped, could implicate supplier eligibility artefacts and subcontractor declarations (ISO, 2020; World Wide Web Development Consortium [W3C], 2023). Each of these developments combine to render a technically possible, procurement-ready, and adjacent DLT-based identity and evidence layer.

The constraining factors are institutional and legal-technical. First, federal-provincial diffusion results in coordination costs: platforms, schemas, and procurement workflows differ, which prevent a contiguous and explicit credentials rail without intergovernmental definitions (Canadian Free Trade Agreement [CFTA], 2017). Second, privacy and administrative-law guardrails require that human reasons, proportionality, and contestability are preserved on any automation or evidential use of ledgers—favoring, vis-a-vis DLT, permissioned governance with auditable access controls over open, public chains. Third, vendor concentration in e-procurement platforms could conduct path dependence (whether high switching costs, proprietary schemas), reducing incentives to pursue open/willing DLT-ready interfaces absent direct formalized approval.

Conclusion, findings and implications: Canada's framework is technologically-agnostic and in a pilot-first vein: it already contains the doctrinal pieces for lawful, privacy-preserving, and cyber-secure blockchain integration (e.g., digital-by-default policy, algorithmic-accountability instruments, privacy regulations) but it needs an operationalization specific to procurement. A credible next step is a framework for an intergovernmental Blockchain in Public Procurement Framework (coordinated by federal and provincial authorities) that (i) authorizes permissioned-DLT patterns (e.g., off-chain personal data; on-chain proofs for timestamps of bid submissions; change orders; confirmations of milestones), (ii) clarifies evidentiary status, and retention for ledger events, in relation to procurement disputes, and (iii) requires inter-agency interoperability

with federal and provincial platforms via standardized credential schemas (capitalizing on ISO/W3C specifications). Without such consolidation, experimentation can remain siloed and logistically peripheral; however, with this, Canada can mobilize disjointed pilots into a system-level integrity upgrade—achieving verifiable traceability while preserving administrative fairness.

3.6.3. Regulatory Approaches of the United States

In the United States, the public procurement landscape regarding blockchain has a decentralized, sector-driven regulatory construct. In contrast with Italy's single authority model, or Canada's coordinated soft-law experimentation, U.S. governance is split between federal agencies endowed with subject-matter authority and the fifty states which have statutory jurisdictions including distinct commercial and archival laws.

For example, at the federal level, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) provide regulation of digital assets, but only to the extent that they act as securities or commodities through the Securities Act of 1933 and the Commodity Exchange Act; the Financial Crimes Enforcement Network (FinCEN) applies the Bank Secrecy Act to anti-money laundering; and the Internal Revenue Service (IRS) regulates tax treatment of digital assets. The regulatory ensemble illustrated above does not provide procurement-specific guidance for ledgers, smart contracts or the process of cryptographic notarization - public contracting is governed by the Federal Acquisition Regulation (FAR), as supplemented by agency-specific procurement directives, which remain technology-neutral (FAR; Securities Act of 1933; Commodity Exchange Act; Bank Secrecy Act).

States - as laboratories of administrative experimentation - are moving faster. Wyoming, Arizona, and Vermont have enacted laws that recognize smart contracts, blockchain signatures or evidentiary presumptions for hashed records. While a number of states have implemented pilots around the use of blockchain for records and credentialing, these pilots are not necessarily consistent across jurisdictions, nor are they often prescriptive on state procurement workflows. This results in an interoperability gap between the different state platforms, as well as the federal acquisition. As a result, while there are publicly funded blockchain pilots in the U.S., the public procurement landscape lacks voluntary, prescribed guidance - a contracting officer considering the use of blockchain has no uniform route to take on admissibility, retention or interface standards. While there are no legislative mandates pertaining to procurement, federal policy and standards organizations have established a basis for potential technologies. NIST's technical reports (e.g., NISTIR 8202) articulate foundational terms — hashing, consensus, permissioned architecture — related to auditability and chain-of-custody; the Office of Science and Technology Policy's (OSTP) request for coordinated approaches to digital assets, including distributed ledgers; and the Federal Data Strategy and OMB Circular A-130, with lifecycle controls, integrity, logging, and interoperability are also important. None of these items create a requirement for blockchain and

they only articulate the parameters for whatever ledger would need to conform to in a federal system (NIST, 2018/2022, OSTP, 2022, Office of Management and Budget [OMB], 2016/2021).

From the standpoint of procurement law, the relevant questions to answer are legal recognition, privacy/cybersecurity, and sovereignty. First, the FAR neither prohibits nor authorizes blockchain, so in the absence of prescriptive interpretive text, contracting officials were unable to determine how they could treat on-chain events (e.g., timestamping bids, attestation of milestones) as documented or permitted records or contractual administration proofs. Second, privacy and administrative law (Privacy Act; APA) duties and federal security baselines prevent majority-given made up of patterns (off-chain personal/commercial data; on-chain proofs), access based on roles and responsibilities, incident reporting, and verifiable chain-of-custody (nearly all the time). Public/permissionless designs are wholly deficient in this regard.

Third, tasking original procurement has in practice been separated from experimentation and innovation: piloting occurs in standards or security communities, meanwhile the procurement workforce has little, if any, model clauses, templates, and cyber security training about ledger evidence and smart-contract assurance. All of these frictions create organizational inertia, and enable merchants to have path dependencies (lock-in to centralized platforms), which is a kind of soft regulatory capture that contributes to the growing trouble we often face while waiting for open DLT-ready interfaces.

Conclusion and implications. The US regime is tech neutral and pilot first and already has the doctrinal pieces to allow lawful, privacy-protective, cyber-secure DLT without needing additional laws. What remains absent is procurement-specific operationalization. A possible way forward is (i) an OFPP guidance memo or Federal Acquisition Circular which specifies when proofs anchored to blockchain will be able to fulfil FAR Parts 4/42 record keeping and administration; (ii) modular, permissioned add-ons to SAM.gov/PIEE/agency systems which will enable bid-timestamp notarisation, supplier-credential verification (VCs), and tamper-evident change-order logs; (iii) workforce enablement (FAI/DAU modules) and NIST aligned interoperability profile (signatures, hashes, metadata). Without this, experimentation will remain marginal and legally peripheral, and with this, the U.S. would be able to translate standards and pilots into verifiable/ reviewable procurement practice flowing from administrative fairness and competition.

3.6.4. Comparative Regulatory Analysis & Discussion

The variation of blockchain adoption paths in public procurement, seen across Italy, Canada, and the United States, reveals differing regulatory logics. In particular, it is observable through the lens of "coding" in Italy. The Public Contracts Code of 2023 establishes a codification-led coordinate for the regulation of procurement through interlinked digitalized processes experienced from end-to-end, layers of certified platforms, and a tier of machine-readable transparency and auditability, with oversight and enforcement vertically integrated through ADAC (procurement

legality/oversight) and AgID (interoperability and technical baselines). While there exist no public procurement instruments which explicitly condition blockchain use, the legal architecture of operation is intentionally cognizable with DLT (distributed ledger technology) features of the rules of the digital regime. All of the features contemplated by the features of the legal relativity are enforceable, especially traceability, auditability, and temporal sequencing of deliverables. As a caveat, Article 8-ter of Decree-Law 135/2018 (as converted by Law 12/2019) states that smart contracts and distributed ledgers may be used subject to thorough identification and time validation thereby allowing a civil law hook for evidential purposes, in future contracting workflows. The eco-system has also been co-dimensioned by EU instruments: Directive 2014/24/EU (for electronic communications) and the eForms regime (Reg.2019/1780) standardize data to permit cross-border comparability; Italy implements them by BDNCP and certified platforms, with tools such as e-CERTIS being for supporting (not required).

Canada is using a federated, pilot-first best-practice approach. Federal policies (e.g., Directive on Service and Digital; Directive on Automated Decision-Making) and provincial initiatives (e.g., verifiable-credential pilots like the OrgBook-lineage projects) contain reference points for modular, permissioned designs, and deportability of data, though there are no procurement-specific, mandatory rules authorizing blockchain functionality. Privacy law (Privacy Act; PIPEDA) and trust/credential frameworks (e.g., PCTF) allow for optional law-compliant DLT uptake, and where there is some without legal compliance. In summary, there is policy coherence without a legally binding obligation that is sufficiently useful for learning and credentials use-cases but slow and cumbersome to scale to core procurement law.

The United States has a high technical capacity but fragmented national procurement systems. Federal regulators (SEC, CFTC, FinCEN, IRS) monitor digital assets (and compliance) systems to procurement, with procurement systems subject to the FAR, which remains technology-neutral and contains no explicit reference to smart-contract execution, on-chain-audit-trail permanency, or cryptographic timestamping of bids. Federal pilots (GSA's Emerging Citizen Technology proofs-of-concept; DHS SBIR exploration) and select state acts (i.e., Wyoming, Arizona, Vermont's evidentiary presumption) fall out-of-sync with federal acquisition rules and legacy systems (SAM.gov/PIEE/FPDS schemas); without FAR interpretive guidance, agencies simply revert to conservative designs; there is no formulation to determine evidentiary treatment of blockchain logs in federal procurement disputes, albeit some states virtualize hashed records.

Privacy/cyber security tension is being managed cumulatively across systems with hybrid architectures (off-chain personal or commercially sensitive information; on-chain proofs), permissioned governance, and rigorous, established, logging/incident management controls. The systems diverge on intermediation at the institutional level: Italy's ANAC/AgID is a legally recognized authority in allocating the legal aspiration to standardize platform requirements; Canada has soft-law-acquired federal/provincial coordination of public procurement through TBS/SSC; and there is a coordination gap with no broker for procurement to connect NIST/OSTP technical specifications, FAR requirements, and workforce practices.

Conclusion. Italy's law-led model achieves legal determinacy and up-front DLT-readiness (without mandating it); Canada's experimental pluralism produces credible pilots with shareable credentialing characteristics but no binding authority; the U.S. showcase its technical feasibility without the legal foundation, generating total implementation paralysis in federal procurement and public procurement models overall. Therefore, transferable reform is concerned with adaptive policy transfer, rather than paying lip service to law (therefore able to embed DLT where a jurisdiction is able to offer (i) admissibility guidance, (ii) profiles compatible with interoperability, and (iii) a competent intermediary willing to facilitate linking innovation/programming technologies with procurement law).

Table 11.Table 3.6.4.1– Comparative Matrix: Blockchain Regulation in Public Procurement

Dimension	Italy	Canada	United States
Regulatory Philosophy	Codification-led; embedded in national legislation and EU directives	Innovation-driven; supported by soft law and policy experimentation	Fragmented and risk-averse; dominated by sector-specific and state-level variation
Governance Structure	Centralized through ANAC and AgID with vertical enforcement powers	Federated model with inter-provincial divergence; TBS and SSC as coordinating actors	Dual fragmentation between federal-state and intra-agency levels
Legal Status of Blockchain	Legally recognized under Art. 8-ter Civil Code and indirectly supported by D.Lgs. 36/2023	No binding legislation; governed by sandbox initiatives and pilot protocols	No federal recognition in procurement; selective acceptance at state level
Procurement Integration	Integrated into certified platforms with risk scoring, traceability, and real-time auditability	Demonstrated in credentialing pilots (e.g., OrgBook BC), but not codified in procurement law	Pilots by GSA and DHS are not institutionalized; FAR excludes blockchain capabilities
Privacy–Blockchain Interface	GDPR-aligned with permissioned architecture and pseudonymization for compliance	PIPEDA and Privacy Act create interpretive tension; hybrid architectures promoted	Privacy Act lacks DLT-specific provisions; compliance uncertain for immutable records
Interoperability & Standards	Mandated through EU interoperability standards (e.g., BDNCP, e-CERTIS)	Voluntary frameworks (e.g., Pan-Canadian Trust Framework); no mandatory standards	No national standard; state-level definitions are inconsistent and non-interoperable

Institutional Intermediaries	ANAC and AgID coordinate legal, technical, and procedural implementation	TBS, DIACC, and provincial authorities coordinate pilots and data governance	No central coordinating body; NIST and OSTP provide technical but not legal guidance
Anti-Corruption Alignment	Formally embedded in anti-corruption law; risk flags and audit trails legally enforced	Referenced in ethical service delivery discourse; not yet institutionalized in procurement law	Not incorporated into procurement law; integrity tools treated as discretionary
Political Economy	EU-funded digital transformation; aligned with Recovery and Resilience Plan	Pragmatic, province-led experimentation with federal coordination incentives	Crypto-centric agenda dominates; procurement innovation receives low legislative priority
Transferability Potential	High legal determinacy; applicable in centralized, compliance-heavy systems	High adaptability; strong for modular policy transfer with customization	Technically feasible, legally incoherent; low potential without structural reform

Table3. 6.4.1 summarizes the key findings from the previous comparison, presenting a structural view of the legal, institutional, and policy facets that outlined path-finding blocks to blockchain uptake in public procurement in Italy, Canada, and the U.S. The table provides not only a summary of descriptive differences but also may be seen as an analytic tool to support the purpose of the dissertation's overarching claim that the feasibility of blockchain uptake is conditional upon a technology's functionality degree and the various overlaps between national legal cultures, governance arrangements, and political economy conditions.

The Matrix first highlights the contrast in approaches to regulatory frameworks. Italy's codification-based approach exemplifies a focus on legal determinacy and procedural standardization found in civil law that allow for the formal embedding of blockchain technology in certified procurement platforms. However, as demonstrated by their blockchain uptake, Canada is also driving a degree of innovation and experimentation, but there are no binding legislative anchors. Finally, the U.S.A. presents the most fragmentary approach; the decentralized risk-averse regulatory oversight is not confined to blockchain patterns; the legal and regulatory risk issues surrounding blockchain technology involves widely divergent corporate ideologies toward regulated and unregulated governance. As noted, there is no commonality evident in either federal or state legislative initiatives toward blockchain integration nor are there normative frameworks evident for supply chain interventions in public procurement.

The next row raises the issue of institutional governance structure where contrasts are critical. Italy's centralized make up (ANAC and AgID) provides a command authority that has a tacit mandate to enact regulatory and technical jurisdictional coordination of public procurement modernization that is aligned with blockchain functionality. In contrast, a federated structure may provide a degree of provincial initiative but the limitations of uneven uptake, lack of regulatory enforcement capacity, and a reduced ability for whole-of-government capacity offers little support for any hope of coordination in Canada.The United States has no unifying agency as a coordinating mechanism, and likely as a result of the isolation between innovation agencies and agencies with procurement responsibility, has institutional inertia, but it would seem, not as a result of technical capacity.

The matrix also depicts differences in the legality of blockchain. Italy can be viewed favourably, with explicit recognition of smart contracts and cryptographic identity mechanisms within its civil code. In Canada and the U.S., these sectors are still exploring subnational or sectoral pilot projects, and lack federal-level procurement legislation that covers the use of DLT in public procurement entirely - which in turn affects the integration space within procurement. Italy’s e-procurement platforms have instituted traceability and audit features as part of their legal procurement process, whereas Canada’s pilots are separate from statutory procurement processes and federally funded pilots in the U.S. are not part of the FAR-based acquisition ecosystem at all.

Privacy governance, standardization, and institutional intermediary roles can also distinguish the procurement regimes. Italy's standard permissioned architecture adheres to and complies with GDPR's provisions, which both enhances Italy's blockchain design legally. Canada and its modular systems stress privacy by design. From a legislative perspective, there remains uncertainty. In the U.S., there is no federal guidance on privacy concerning blockchain, which leads to institutional reticence. Italy stands apart from both Canada and the U.S. in that only Italy has an enforceable anti-corruption alignment, whereby it has embedded blockchain-enabled integrity in the legal procurement framework. Currently such systems only represent speculation and marginal results in Canada and the U.S. respectively.

Lastly, the matrix emphasizes the transferability of each model. Italy offers a useful starting point in a centralized, compliance-oriented jurisdiction for jurisdictions/areas seeking to embed blockchain in statutory procurement systems. Canada's modular, sandbox-based system offers adaptability for jurisdictions that prefer soft methods of coordination over formal procedures. The central theme of the U.S. climate suggests that although U.S. government pilots appear to be technically sophisticated, if there is absence of effective legal coherence and institutional intervenor roles, it is unlikely that regulatory fragmentation can lead to implementation.

In summary, Table 6.4.1 is the implementation of the concept which formed the core framework of the dissertation by translating theoretical differences into institutional comparison diagnostics. It demonstrates the argument within this paper: that the fundamental aspects for effective integrating blockchain into public procurement is intertwined with the meta-regulatory

architecture's aspects highlighted in this paper, with respect to the reliability of legally enforceable contract, the capacity for procedural interoperability, and the relative political will within their own jurisdiction.

3.7. Corruption Vulnerabilities & Blockchain Solutions in Public Procurement

Public procurement involves large financial flows, heterogeneous actors, and sequential decisions with obligatory timelines. In this type of environment, the typical corruption risk can be anticipated where there is high discretion, asymmetric information, and weak auditability. Then, any anti-corruption framework must first uphold the integrity of processes over the entire procurement lifecycle before it can attempt to target specific points of manipulation. This subsection links junctions with high corruption risk—planning, tender design, bid submission and evaluation, contract award, project implementation, and audit—to blockchain controls that change the strategy set available to corrupt actors. The intent of this subsection is not to claim blockchain "solves" corruption, rather specific functionalities—tamper-evident ledgers, cryptographic commitments, deterministic execution, and accountability linked to identity—can remove the tangible levers which most schemes depend on, so long as they have been designed legally, permissioned, auditable (Weingärtner et al., 2021; Torkanfar et al., 2023).

Lifecycle mapping and control effects. In the planning step, budget overages or politically influenced project selection remain common due diligence violations because justifications, revisions, and approvals are widely dispersed and can easily be overwritten. A permissioned ledger that documents justification, versioned attachments, and approvals (with digital signatures linked to role-based, verifiable credentials) creates a non-repudiable sequence of events; ex-ante commitments may also be tested ex-post, while out-of-sequence additions stand out in the evidence (Monteiro & Correia, 2023; Andreasen et al., 2018). In terms of tender design, "specification steering" continues to fetter accountability through secret edits and back-dating. Publishing machine-readable public notices or on-chain hashes of the notice corpus ends ambiguity on what was disclosed, at which time, and by who; it may also provide access-controlled authoring workflows and implementable smart-contracted state transitions to verify author, approver and timestamp on every change (Diadia et al., 2022).Recording and evaluating bids are common considerations, including the canonical levers of pre-disclosure, colluding and colluding or manipulating scores afterwards. Here, blockchain's original offering is to decouple confidentiality from competition and verifiability from a later time. Sealed-bid protocols can timestamp on-chain commitments while obscuring the content of the bids until after the deadline has passed. Some practical constructions implement the commitments alongside threshold decryptions or multi-party computations that serve to prevent a single official from early interpreting the bids, consequently

making the eventual unveiling of the bids—a problem many cleanly tend to—provably accurate; next steps in the evaluation algorithms then cleanly deterministically executes once opened so there is a reusable trail from the inputs to the rankings (Baranwal, 2020; Li et al., 2021; Weingärtner et al., 2021).

On award, the inverted opaque reversals and shadow negotiations can be dissuaded by coding the bid to award pipeline as a verifiable state machine. The awarded contract would be complete as a computable function of the evaluations, and departures from that award—given that they are not based on a lawful recorded ground of any sort that are open to audit—will be by design suspicious. Smart-contracting the issuance of the award document so that it is hash linked to the tender and evaluations artifacts will not reduce the attack surface for silent substitutions, but will certainly preserve the basic legal protections and controls such as explicit “pause/override with reason” steps adequately identity bound (Torkanfar et al., 2023). During the implementation phase of a project, losses can compound due to inflated change orders, unprovided quantities and/or delayed payments for selected lines. By representing milestones as on-chain states and only releasing payments contingent on a defined attestation by the contracting authority, supervisor, and where possible, retained third parties such as through an IoT signal or notarized delivery event, implementation is conditionally guaranteed to their verifiable performance and significantly raises the cost of "papering over" the differences (Weingärtner et al., 2021). Finally, audit failures typically result from incomplete, mutable, or siloed records. Running a ledger that chain bids, bid commitments, evaluation proofs, awards, amendments, deliveries, and payments establishes verifiable, end-to-end traceability, with cryptographic continuity; all forensic questions—who changed what, when, under what authority—are answered by system design rather than reconstructed effort (Weingärtner et al., 2021; Diadia et al., 2022). During this process, permissioned platforms (e.g. Hyperledger Fabric) maintain confidentiality and access control without compromising audit-grade provenance (Androulaki et al., 2018).

Typologies of corruption and targeted countermeasures. The literature supports a functional division of procurement corruption into: (1) political manipulation with agenda setting; (2) bid-rigging and collusion; (3) favoritism and nepotism; (4) record falsification; (5) delivery fraud; and (6) audit circumvention. Blockchain addresses these categories as follows. Political manipulation is minimized only when early justifications, trajectory of budgetary conditions, are locked in, and (where governance models do not prevent) there is distributed validation, or endorsement by multiple parties (Benítez-Martínez et al., 2022; Ibrahimy et al., 2023). Bid-rigging is addressed by sealed-bid commitment schemes, alongside privacy-protected evaluation schemes, which decouple confidentiality from post-hoc verify-ability (Baranwal, 2020; Li et al., 2021). Favoritism within award exists theoretically by coupling deterministic, transitory pathing from the evaluation outputs into the award, and premises of accountable override gates (Torkanfar et al., 2023). Record falsification is structurally deterred by immutable, hash-chained versioning (Diadia et al., 2022; Batista, 2024). Delivery fraud is avoided through milestone-triggered disbursements linked to verifiable attestations, and, where additions to the tracking process are entirely appropriate,

exogenous proofs (Li et al., 2024). Audit circumvention defeats multitude accountability choices by establishing continuous, end-to-end, anchor-based, identity-traced paths that dramatically reduce innate trust in mutable enterprise logs (Sousa, 2023; Trequattrini et al., 2023).

Design warnings and technical limitations. Two main caveats are repeated. First, the notion of sealed-bid confidentiality can be earned but is not guaranteed: correctness-of-opening and unilateral decryption resistance are dependent both on tempo and the protocol itself (e.g., commit-reveal with threshold decryption protocols or MPC-derived protocols), and of course the ease of key management (Baranwal, 2020; Li et al., 2021). Second, while it is not necessary, "code is law" has no place in public procurement. Smart contracts could enforce process, like deadline and logging, or role limitations, whilst keeping the legally accountable discretion with explicit and auditable overrides acting on behalf of other parties judicating (Torkanfar et al., 2023). These constrain the architecture, and bring blockchain's strength—for traceability, non-repudiation, and automation—to the requirements from administrative law, for reason-giving and review.

Institutional and legal conditions. Sustainable reform embraces circumstances outside of pure technical feasibility. Jurisdictions are challenged settle on structural and legal limitations, like regulatory fragmentation—which creates a legal gray area for the procedural and evidentiary status of smart contracts and decentralized records parties, particularly where procedural codes instruction procurement process (prescriptively) and the utility of judicial practice utilizing evidence produced from blockchain (Sava & Dragos, 2022; Kálmán, 2024; Bustamante et al., 2022). The Italian case study offered research context-specific to Italy, detailing how usage of blockchain for anomaly-exclusion, the immutable evaluation record, or even the decentralized ledger could function with centralized oversight. These were prototypes dissolved with the (not) intent of confirming production deployments, but in alignment with Italian framework (Bouaicha et al., 2024; Batista, 2024). Canada, which has a relatively strong digital-governance ethos, faces multilevel procurement authority; pilots referenced in the literature mainly stress conceptual readiness or adjacent domains to which they relate, and usually finish declaring enforceability and interoperability being open questions (Kálmán, 2024; Sava & Dragos, 2022).In the United States, regulatory diversity enables bottom-up experimentation; peer-reviewed prototypes like BidChain in construction tendering show practicality, while raising concern for the need for stronger, cross-jurisdictional clarity of the legality of smart contract, and how to handle interoperability between agencies (Torkanfar et al, 2023; Bustamante et al, 2022). Across contexts, preconditions reoccur: process-specific, jurisdictional legal reform to acknowledge blockchain records and automated steps; public sector capacity building and change management; pilot spin-off and modular implementation of high-risk industries; community stakeholder engagement or social license models grounded in disclosure and transparency mandates (Sousa, 2023; Mahula et al, 2022; Wadegaonkar et al, 2024; Colque-Diaz et al, 2024; Batista, 2024).

Risks and limiting factors. Literature cautions against digitizing processes without re-designing governance, as the discretion will just be encoded into policies - platforms can either create contingencies of centralization, or obfuscate accountability if the terms of participation, access, or

override are not (de)constructed (Bustamante et al, 2022). Over-determined smart contracts may conflict with doctrines that should incorporate interpretation, negotiation, or equitable adjustment - procurement law will in any case require humans-in-the-loop with reason-giving, even with automated execution (Sava & Dragos, 2022; Kassen, 2023). Scalability and environmental concerns favor social consent - public accountable systems must ensure they can process high throughput with durable storage whilst minimizing energy cost, which also favors permissioned architecture and layered architecture (Sobolewski & Allessie, 2021). Privacy-transparency trade-offs after numerous iterations remain present, and competitive tendering; cryptographic mechanisms (such as zero-knowledge proofs, differential access) may minimize some tension between the commercial interactions and the public accountability principles, but cannot remove the tension (Siddiqui et al., 2023). Lastly, lock-in of vendors is essentially a governance risk; again, open standards and theoretical possibilities of individual open modules reduce the risks of single dependence while also allowing flexibility over longer time-frames (Ba et al, 2023; "Dematerialization of Public Procurement...", 2022).

Synthesis and contribution. The collected evidence creates a clear, defensible claim: blockchain does not remove corruption in procurement, but embedded into lawful, permissioned, and contended structures it does re-distribute discretion - renaissance from hidden, ex-post rationalizing accounts to transparent, ex-ante rules and verifiable events. As lifecycle mapping illustrates, cryptographic commitments, deterministic calculation, and provenance typically tied to identities address specifically touchpoints at which discretion is manipulated, as the typological analysis illustrates the types of corruption most effectively dissuaded. The comparative perspective illustrates success is not just a product of technological readiness, but also takes into consideration institutional combinations; legal recognition of automating processes, coordinated governance across the levels of the government, capacity building and pilot spin-offs. The next subsection expands on this claim by exploring jurisdictional regulatory initiatives, and institutional conditions enabling the (scaling or not) of those conditions in "Italy, Canada, the USA" (Sousa, 2023; Kálmán, 2024; Bustamante et al, 2022).

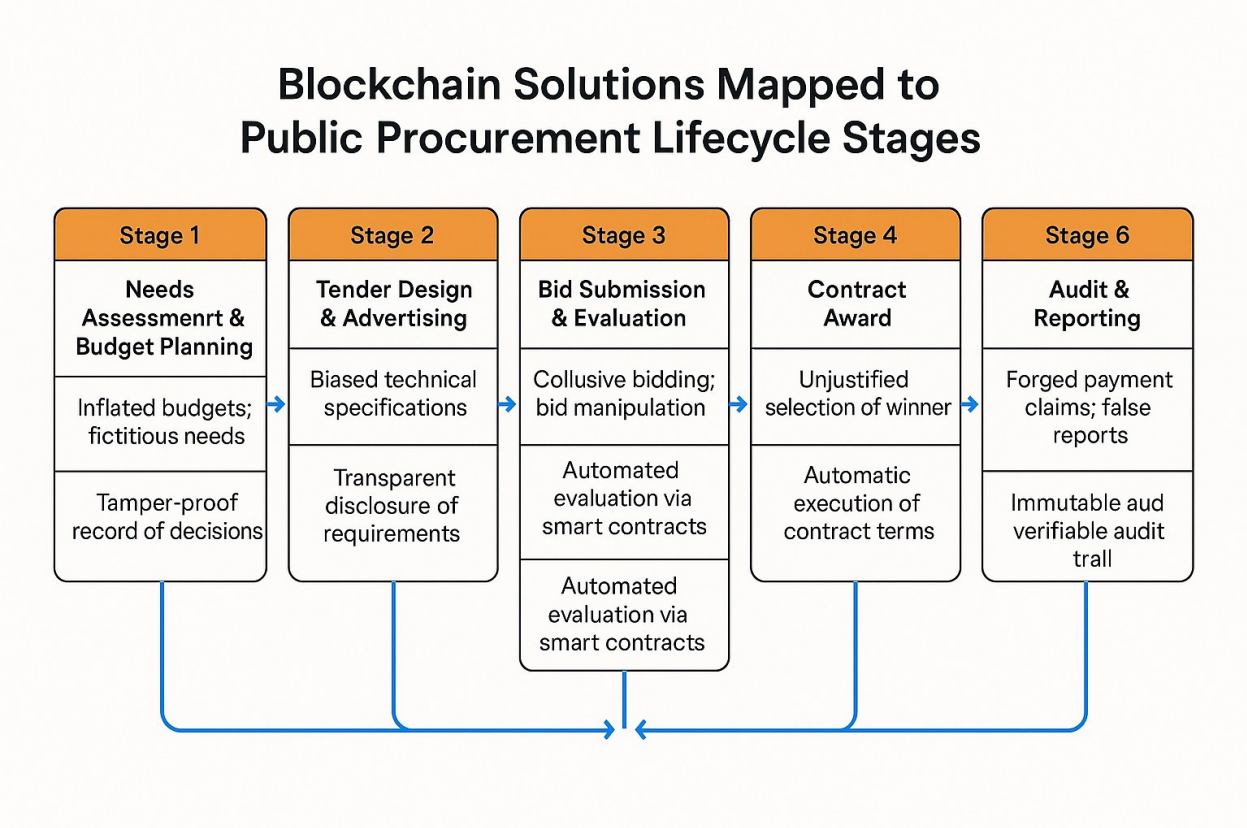

Figure 8. Blockchain Solutions Mapped to Public Procurement Lifecycle Stages

Figure note. The figure3.7.1.1 illustrates controls at the process level (immutability, cryptographic commitments, deterministic execution, identity-bound actions). It is a design mapping, not evidence of jurisdiction-wide deployment.

Figure 6.1.1. Blockchain Solutions mapped to public procurement lifecycle stages. This figure provides a mapping of six conducted stages in procurement with associated blockchain controls aimed at addressing corruption risks at each stage. In Stage 1 (Needs Assessment & Budget Planning) procurement officials can use tamper-proof, time-stamped records to mitigate the odds of inflated scopes of work or fictitious needs. Stage 2 (Tender Design & Advertising) processes tenders with records of notices and criteria on the legers can enhance transparency for disclosure, as well as facilitate or enforce, machine-readable versions. In Stage 3 (Bid Submission & Evaluation) officials can use an allocation process to open bids sealed before the submission and deterministic decision or evaluation with auditable files to avoid collusion and manipulation of the scores. In Stage 4 (Contract Award) the awarded contract will be referenced to the evaluation outputs without arbitrary accountability for steps overriding sealed knowledge, thus limiting unjustifiable selections. In Stage 5 (Contract Implementation) delivery milestones and change orders can be on-chain to represent disbursal contingent on verifiable attestations. Stage 6 (Audit & Reporting) provides an immutable and verifiable audit trail for integrating tenders, bids,

evaluation files, awards, amendments, deliveries, and payments and can support continuous operability oversight and ex-post reconstruction.

3.7.1Technological Feasibility and Current Approaches in Italy

The technological feasibility of using blockchain in public procurement in Italy must be interpreted in relation to the general path of digitalization of administrative processes in the country. There is a pronounced consensus in the literature that currently existing interfaces of e-procurement and dematerialization represent an adequate ecological niche for permissioned ledger functions, given that implementation is sequenced, performance is measured, and governance is specified (Bouaicha et al., 2024; Ba et al., 2023; Wadegaonkar et al., 2024). In this context, experts did not view blockchain as simply supplanting procurement information systems rather as a new layer that would maintain integrity for audit and verification in existing proportionate digitized processes (Cuny, 2022; Siddiqui et al., 2023).

In terms of digital infrastructure readiness, researchers have found that those procurement systems which have existing electronic interfaces and structured data publications are most likely to successfully evolve with the incorporation of some distributed ledgers for selective high-end functionality, for example in supporting tamper-evident logging and in standardizing record custody (Cuny, 2022; Treiblmaier & Sillaber, 2020). In empirical investigations of demonstrator deployments using enterprise frameworks — most notably Hyperledger Fabric — and sometimes Ethereum-compatible smart-contract layers, there was evidence of technical operability across scoped modules including evaluations of tenders, verifications of milestones, and open-contracting format aligned publication (Ba, 2022; Čeke et al., 2022). At the same time, despite being able to find evidence of demonstrator deployments, the literature remains replete with accounts of continuing heterogeneity of connection, compute, and IT resourcing and staffing across regions, as well as with many of the smaller municipalities, these are seen to be persistent structural obstacles to achieve full scale and uniform utilization (Bouaicha et al., 2024; Baima et al., 2024).Lack of consistently reported national benchmarks for latency, throughput, and availability under procurement-grade loads leads to assessments being case-bound rather than transferable (Sobolewski & Allessie, 2021; Allessie et al., 2019). The evidence encourages a phased approach to embedding blockchain first at integral integrity checkpoints and increased later as capacity develops at the network and organizational levels (Ananthajothi et al., 2024; Piccardo et al., 2024).

Cybersecurity posture and hosting readiness are repeatedly cited as vital enabling factors. While ledger immutability and public-key infrastructure (PKI) are necessary conditions, they are not sufficient by themselves, with risk being concentrated on endpoints, identity and access management, and integrated layers that link legacy systems with smart-contract logic (Siddiqui et al., 2023; Wadegaonkar et al., 2024; Ramya et al., 2024). The literature is therefore advocating for blockchain-specific security frameworks with robust digital identity, node-level access control, fraud prevention analytics, and verifiable software-lifecycle processes specifically designed around procurement use cases (Pokharel & Kshetri, 2024; Sousa, 2023). Reflecting on hosting, the

literature reviewed presents a fragmented view of assessed capacity; while centralized cloud (computing) is adequate for pilots, resilient operation of procurement archives and verification services is favored by distributed or edge-proximate storage—for example, addressable content using IPFS-type repositories—but will still be bound by legal and assurance requirements around data custody in the public sector (Bouaicha et al., 2024; Sobolewski & Allessie, 2021; Torkanfar et al., 2023). Along the lines of sources, authors also highlight a lack of coordinated and blockchain-specific cybersecurity integration for public administrations; resulting in many initiatives remaining at the experimental level and not improving institutional confidence for scalability (Wamba et al., 2024; Sánchez-Graells, 2024). Amidst these considerations of infrastructure and security, Italian pilots have an evidentiary usefulness. Demonstrators show that smart contracts can automate compliance gateways, enforce procedural rules, and provide immutable, auditable records across aspects of the procurement lifecycle when the domain is unbounded and governance in clear (Ba, 2022; Čeke et al., 2022; Ba et al., 2023). Reported use cases can range from dematerialized tender evaluation as working in compliance with open-data standards, to manipulated anomaly exclusion logic within the record layer of the project, or even the automated confirmation of contractual milestones (Bouaicha et al., 2024; Ba, 2022). Other examples from subnational players have demonstrated how empowering regional actors with budget autonomy is an effective method to foster experimentation, but it also demonstrates how obstacles to horizontal replication can be revealed where actors have different levels of agriculture digital maturity and platform architectures (Treiblmaier & Sillaber, 2020; Sobolewski & Allessie, 2021). Pilots tend to have reporters and parallel systems with incumbent platforms, this preserves continuity but also has the potential for redundant processes in processes are not interoperable when they should already be implicit in the design stage (Cuny, 2022; Piccardo et al., 2024).

The situated technical challenges arise at the seams when distributed architectures confront administrative realities. Data transfer to bolstered subsystems necessitates prescribed processes for evidentiary resilience, legal standing, as records transfer from a central repository to content-addressed / ledger-anchored storage with respect to the trackable nature of all relevant elements including provenance, timestamping and chain-of-custody for public record keeping (Torkanfar et al., 2023; D'Avanzo, n.d).Interoperability is also fundamental; means to align with EU procurement data standards (e.g., ESPD) and parallel international publishing schemas such as the Open Contracting Data Standard (OCDS) will be required both to avoid siloed ledgers and duplicate interfaces and to ensure the ledger layer amplifies the pre-existing e-procurement ecosystem rather than fragments it (Ba, 2022; Cuny, 2022). On scalability, the literature warns that public or semi-public networks may create latency and energy-costs that we will have difficulty reconciling with high-volume tendering and time-boundedness. Permissioned architectures utilizing Raft ordered processes (the predominant configuration in Fabric) or, in necessary use cases, BFT variations, can lower time-to-finality and administrative costs – subject to governing validator sets and the auditability of all administrative functions (Wadegaonkar et al., 2024; Ba et al., 2023; Sousa, 2023). The tradeoffs in architecture also connect to legal issues about evidentiary status of records produced by blockchain, and enforceability of smart contract logic in public law

contexts, which continue to dampen institutional appetite to replace legacy systems instead of complementing them (Sava & Dragoș, 2022; Kálmán, 2024; Curry, 2024).

Energy use is part of the same feasibility calculus: while the improvements regarding consensus systems lessen the energy use usually attributed to public blockchains, the literature considers energy a design and policy variable to be addressed early while choices are being made regarding architecture, performing tests, and in green-ICT procurement specifications (Sousa, 2023; Čeke et al., 2022).In permissioned deployments of administrative ledgers, the authors find clear benefits to transaction finality and resource utilization in cases where smart-contract modules are properly sandboxed and profiled so automated checks will not add unreasonable time to competitive processes (Ba, 2022; Siddiqui et al., 2023; Bouaicha et al., 2024). The performance–assurance balance is associated with a larger governance aim: transparency, accountability, and sustainability, which a number of contributions associated with the potential of traceability for ethical and green procurement where indicators and data-publication interfaces have been designed for comprehension by diverse constituents (Giamberardino et al., 2024; Gomez-Trujillo et al., 2021; Wadegaonkar et al., 2024; Siddiqui et al., 2023). As technical feasibility depends on organizations to adjust priorities, literature focuses on institutional capacity and socio-political tensions. Institutional leadership that gets procurement, legal, and IT units aligned; owns its data and processes; and uses effective risk management practices under the scrutiny of public accountability provides the cleared path sought to move past pilot projects (Haq et al., 2024; Treiblmaier & Sillaber, 2020; Curry, 2024). Disruption across national, regional, and municipal government causes an added level of complexity in uniformly adopting blockchain practices, thus warranting the case for national-level standard-setting, certification regimes, and reference implementations for local administrators to build upon without recreating the core integrated components (Cuny, 2022; Sánchez-Graells, 2024). Participation as part of EU-level infrastructures and programs (e.g., standards development, cross-border interoperability activities) presents scaled economies for shared learning, coupled risk in integrations, and explicit assurance expectations regarding permissioned administrative ledgers (Sousa, 2023; Ba et al., 2023). Authors also caution transparency is not automatic—the public value is mediated by interface design; data intervals published; and user ability to assess what it published in public domains, particularly for SMEs and civil-society monitors (Piccardo et al., 2024; Kademeteme & Bvuma, 2023; Kshetri, 2021; Maolani, 2024). Just as technological characteristics are essential, addressing human-factors considerations is equally important in securing the governance returns that motivate the motivation to act.

In conclusion, systematically the evidence describes an Italian context possible with technically feasible, localized, permissioned blockchain uses in procurement, and that there are specific pathways for all future developments if integration, assurance, and governance are specified as carefully as the ledger features. Specifically, our assessment indicates: (i) areas of the administration currently have a base of digital infrastructure that is suitable for an anchor ledger to record the audit-relevant events; (ii) pilot testing has taken place and validated the core functions

in controlled environments; (iii) there are tractable technical challenges—and reasonably accurate assumptions about the quality of the data—that are involved with data migration with evidentiary continuity, an OASIS-style standards-first interoperability approach (using EU standards, such as ESPD, and international schemas, such as OCDS), consensus and hosting type choices that mesh with the administrative workload, and energy-awareness in performance engineering—that could reasonably be overcome with coordinated institutional will and legal clarity to provide a different perspective in subsequent project considerations (Ba, 2022; Čeke et al., 2022; Bouaicha et al., 2024; Sava & Dragoș, 2022; Sousa, 2023). In summary, the subsection was able to contextualize its objectives through (i) contributing to Italy's readiness profile; (ii) synthesize evidence from demonstrators; (iii) relate barriers and opportunities to the project considerations—including socio-political tensions—arguably funneled into informing the chapter's annotated purpose to specify a scalable, standards-compliant, and security-assured pathway by which blockchain can help facilitate more integrity, transparency, and efficiency of the Italian public procurement system, without sacrificing legal certainty or administrative reliability (Siddiqui et al., 2023; Wadegaonkar et al., 2024; Ba et al., 2023).

3.7.2 Technological Feasibility and Current Approaches in Canada

In Canada, the public sector's technological feasibility of blockchain adoption is the result of interaction among institutional experimentation, infrastructure readiness, and boundaries inherent in the technology and organizational contexts of use. In the past decade, uses of blockchain technologies for Canadian initiatives have been focused on advancing operational transparency, automating bureaucracies and enabling trust in government organizations (Zelenski, 2024; Abelseth, 2018; Reddick, 2021)—across green financing, digital identity, wholesale DLT for payments and securities, and regulated supply chains. The range of projects indicates a collective approach towards capitalizing on opportunities to improve the efficiency and effectiveness of public service delivery: the Canada Greener Homes Grant is an example of the use of a distributed ledger to facilitate disbursements and improve auditability. Availability of blockchain for supply chain verification can also be observed in replica-provenance networks using permissioned networks for cannabis traceability, which resulted in regulatory compliance and product proof (Abelseth, 2018; Zelenski, 2024).

While pilots have illustrated pragmatic uses of blockchain technology in Canada, foundational work has been done in multi-phase exploratory work focused on regulatory permissible DLT networks—for example, Project Jasper informed DLT and centralized network options for large-valued payments and securities settlement, exploring central bank digital currency designs and blockchains with data privacy and permissioned participants (Reddick, 2021; Choi et al., 2021; Veneris et al., 2021).

Digital identity has been a further area of exploration in Canada. Verified.Me has been described as a consortium-governed identity network whose purpose is to provide a user-centered approach

to credentials, exchange of verified credentials between institutions while protecting privacy (Boysen, 2021; Wolfond, 2017). Nevertheless, organizational inertia, variable capacity and infrastructure, and data governance remain impediments to adoption demonstrating that innovations in identity systems must be closely connected to broader interoperability and policy regimes (Boysen, 2021; Murphy et al., 2021).

Several technical issues impact scalability and institutionalization. Interoperability with legacy information systems is central, as many existing databases and services in government are not easily integrated with distributed ledger protocols and, as noted in the literature, there are few if any available standardized middleware to bridge blockchain with legacy architectures, notably in data-heavy areas such as health and taxation (Dziundziuk & Dziundziuk, 2022; Radonjić et al., 2024; Cadoret et al., 2020; Owens & Hodzic, 2022). Canadian scholarship routinely nests these issues in policy-aware designs, such as health data models that use dispute-evidence audit trails and have explicit consent and ethics exchange processes, as well as governance structures that feature legal defensibility, data privacy, and accountability (Cadoret et al., 2020; Mustafa et al., 2024). At the same time, policy fragmentation in regulatory environments and mixed digital maturity in how even departments and regions approach blocks and blockchain technology has created uneven development, with progress in finance, identity, and green finance not benefiting public sectors like health and public health surveillance (Murphy et al., 2021; Mansour et al., 2024). Rapidly evolving protocols for technology selection under diverse profiles, such as scalability, privacy, consensus, and dependency on vendor lifestyles, adds another layer of complexity that has also contributed to the risk-averse behavior of organizations. Relatively little available synthesized literature exists to guide the choice of protocol in the field of public administration, and this is likely to perpetuate cautious organizational behavior (Zelenski, 2024; Radonjić et al., 2024; Batubara et al., 2018; Dziundziuk & Dziundziuk, 2022).

Scalability is also still a real concern, notably for permissioned networks. The transactional throughput and interoperability with other networks may not hit the high standards required to support the real-time, large capacity services required by national frameworks for tax, national registries, or procurements. The proposed remedies prioritize technical optimization and hybrid strategies that allow ledgers to live with legacy systems while gradually taking ownership of higher-impact activities (Murphy et al., 2021; Wibowo & Yazid; n.d.). Collaboration with research organizations and policy professionals is more visible, both in green financing pilots and in central bank digital currency (CBDC) design. This signals a maturing ecosystem for knowledge co-production examples for designing technical solutions within statutory and policy constraints (Zelenski, 2024; Choi et al., 2021; Veneris et al., 2021). In the public sector, the momentum for digital tools is correlated with expectations for transparency, auditability, and inclusion. The potential benefits of blockchain's immutability and traceability, in combination with privacy protections, have become increasingly central (Ruap & Sultana, 2024; Piccardo et al., 2024; Elisa et al., 2020; Mustafa et al., 2024).

The heterogeneity of stakeholders also affects feasibility. Central agencies with nation-wide scope will generally converge towards privacy-preserving and interoperable options, while smaller more narrow agencies serving a specific sector may prefer narrower architecture aimed at a specific set of regulatory outcomes (Reddick, 2021; Abelseth, 2018; Zelenski, 2024). The inconsistency in public authorities and private authenticators encourages different priorities and key performance indicators- compliance and reliability versus speed and proprietary features- which combine to limit procurement and standardization and create difference in maturity of pilots (Bustamante et al., 2022; Mustafa et al., 2024). The tensions that exist between transparency and privacy are not unique or new. For example, tamper-evident records help to combat opacity, but the public's desire for immutability directly contends with existing laws and policies that require people the right to rectify and erase. The literature highlights privacy-enhancing practices such as selective disclosure and cryptographic proofs, all of which seek to align privacy requirements with the Privacy Act in Canada (Mustafa et al., 2024; Radonjić et al., 2024; Elisa et al., 2020; Yuan et al., n.d.). Following the trajectory of administrative accountability, current government deployments suggest a preference for permissioned or consortium models to limit access and ensure finality. While these models promote verifiability and oversight, they can hinder the potential for broader scalability and interoperability across jurisdictions (Boysen, 2021; Reddick, 2021; Wolfond, 2017).

Sustained feasibility is predicated on transcending pilot and silo scenarios. It is against this backdrop that the literature recommends interoperable governance models that allow for modularity for sector-specific applications, within Canada's national purview for coordinated care, so as to limit parallel, incompatible systems per jurisdiction (Dziundziuk & Dziundziuk, 2022; Wibowo & Yazid, n.d.). Related frameworks identify enablers and barriers across organizational and technical dimensions and represent domains such as e-taxation, e-health and inter-agency exchanges, where notable affordances and constraints exist (Falwadiya & Dhingra, 2022; Owens & Hodzic, 2022; Cadoret et al., 2020; Murphy et al., 2021). Specifically, to healthcare, British Columbia has forthcoming proposals of transparent sharing protocols, consent management and trust structures; however, success depends on bridging human infrastructure--leadership, policy consensus, and organizational culture--technology needs to be integrated into the capacity building charter (Cadoret et al., 2020; Murphy et al., 2021).

Alignment with the e-government agenda centered on automation, accountability, and participatory service delivery model limits feasibility. The more conceptual governance models envisage lifetime, traceable, and citizen-mediated interaction, while empirical work evidence opportunities to improve data accountability and reduce bureaucratic friction (Kassen, 2024; Ruap & Sultana, 2024). Maturity models suggest a lot of implementations remain within pilots or proof-of-concept phases and little longitudinal evidence and architectural production-level investment is available (Wamba et al., 2024; Bustamante et al., 2022). Regulatory uncertainty—especially around data ownership, liability, and auditability in distributed contexts—exacerbate risk-tolerant attitudes, and complicate trans-jurisdictional replication (Selvanesan & Rodrigo, 2024). The literature flags the need for governance frameworks that include legal accountability, privacy

protections, and technical compliance; without these, project-plateaued forms of decentralization do not scale easily only across departments and/or provinces (Mustafa et al, 2024; Wibowo & Yazid, n.d.; Yuan et al, n.d.; Boysen, 2021; Bustamante et al, 2022).

Inflating decentralization and a hierarchical administration structure is a real challenge for design, and hybrid models - permissions-ledgers that the authorizes can designate validators or transaction processers - allow compromise by ensuring audibility and oversight, although they will turn conservativism, and thus reduce the possibility for innovation from systemic to incremental change, appears to be the compromise (Batubara et al, 2018; Dziundziuk & Dziundziuk, 2022). Cases studies in public finance that have examined ledger as an implementation of governance decision making will explain strengthening the potential of fiscal transparency was a natural feature of the ledger as long as the evaluation took place post-deployment, after important contextual considerations (Varada et al, 2021; Zelenski, 2024). Academic research also recognizes the unrealized possibilities of shared infrastructure layers to encourage horizontal co-ordination and co-delivery of services, but this relies on technical enabled systems where participating partners / organizations are willing to create new unbundled arrangements from working within multiple institutions for with embedded legacies (Kademeteme & Bvuma, 2023; Ruap & Sultana, 2024; Radonjić et al, 2024). There is limited knowledge from citizens exposure to the wider of blockchain in all the studies, emphasizing the need for public education and participatory design, to maintain legitimacy and understanding of collaborative opportunities for formatting ledger enabled processes (Piccardo et al, 2024, Mills et al, 2023).At a policy level, the literature notes the proliferation of disjointed trials facilitated without a concept of federal engagement, which may leave many possibilities for shared infrastructure and shared standards unexploited (Bustamante et al., 2022; Maragno et al., 2021). Within the discourse of CBDCs, the content specific to Canada tended to focus on privacy and legal compliance, while technical roadmaps, and cross-border operability lacked detail (Choi et al., 2021; Veneris et al., 2021; Alexopoulos et al., 2021; Selvanesan & Rodrigo, 2024). More broadly, conceptualizing blockchain as applied to public services is encumbered by limited performance measurement and longitudinal tracking; the literature specifies the need for systematic monitoring, independent audit, and user centric feedback where efficiency and transparency are claimed (Meyers et al., 2022; Cagigas et al., 2021). Furthermore, technical immaturity impedes evidence-based conclusions, and data standardization, throughput, and energy production were noted as limitations in intensive data situations for which risk-aware pathways have been constrained to incremental adoption with aspirations toward consideration of energy efficient architectures as sustainable governance for digital technologies (Halim, 2023; Batubara et al., 2018; Zelenski, 2024). Last of all, digital equity was highlighted as a structural foundation: blockchain initiatives might unintentionally exclude the populations most reliant on public services if the inequities of infrastructure literacy are not asserted attention to - this was especially relevant to rural, remote, and Indigenous communities (Murphy et al., 2021; Leborgne, 2023; Wamba et al., 2024).

Together, feasibility in Canada is best understood as layered and dynamic based upon the maturity of protocol, institutional arrangements, legal congruence, inter-institutional coordination, public literacy, and social inclusiveness. The literature fits into practical outcomes: (i) coordinated guidance to interlink standards for technology needs and adoption across jurisdictions; (ii) opportunities for public-private-academic partnerships amongst high-impact use cases; (iii) community designed modular systems with both federalism and enforced security and interoperability; and (iv) embedded ongoing monitoring, ethical deliberative frameworks, and public engagement to foster robust credible evidence and legitimate sustainability (Selvanesan & Rodrigo, 2024; Bustamante et al., 2022; Zelenski, 2024; Boysen, 2021; Choi et al., 2021; Dziundziuk & Dziundziuk, 2022; Radonjić et al., 2024; Varada et al., 2021; Owens & Hodzic, 2022). Thus, in this path forward as a coordinated governance structure with capacity building, blockchain can shift from pilot experiments to resilient, scalable, equitable infrastructures for public administration practice in Canada when coupled with technical design.

3.7.3Technological Feasibility and Current Approaches in the United States

In evaluating the technological feasibility of blockchain to address anti-corruption in the U.S., it is essential to consider feasibility as a socio-technical construct rather than simply an engineering problem. In high-risk contexts, like public procurement and land records, the canonical affordances of blockchain—immutability, traceability, and automation through smart contracts—map well to integrity objectives of tamper-evident logging, auditability, and easing discretionary bottlenecks (Ølnes, Ubacht, & Janssen, 2017; Clavin, Duan, Zhang, Felten, & Narayanan, 2020). However, and subsequent to piloting, moving onto an institutional capability for using blockchain for anti-corruption, is mediated by organizational routines, workforce capacity, and intergovernmental coordination, all of which nuance the technological anti-corruption potential at H2 (mitigation through transparency/immutability) and conditions the comparative performance at H3 (U.S. technological advantages in a structurally-fractioned context).

The U.S. context, defined by a mature digital infrastructure and standards ecosystem together with a federal architecture that accelerates experimentation and complicates scaling, is important to note. There are some tangible federal guidance and reference architectures, such as the NIST blockchain overview and NIST cybersecurity practice guides, which not only clarify processes for implementing permissioned blockchains, but offer guidance on secure configuration, cryptographic hygiene, and role-based access to data (National Institute of Standards and Technology, 2020; Howard & Vachino, 2019). Each of these design elements relates specifically to anti-corruption objectives, for instance, permissioned ledgers can offer opportunities for fine-grained participation in data use; provenance-preserving data modeling; and verifiable workflows, each of which could help mitigate opaque interventions during procurement or registry updates (Clavin et al., 2020; Ølnes et al., 2017). At the same time, federalism produces heterogeneous adoption trajectories across agencies, states, and levels of government. Diffusion theory asserts

that credible demonstrations will create mimetic and normative pressure on peer institutions, but it also predicts variation given that resource endowments, legacy systems, or professional networks differ (Rogers, 2003; DiMaggio & Powell, 1983). So far, the result of this duality has been a landscape of promising pilots and wide-ranging institutional preparedness.

From a technical perspective, three tendencies for feasibility matter for adoption. The first is scalability and performance: permissioned platforms generally nominated for public-sector deployment can offer deterministic finality and controlled transparency, but will encounter throughput and latency challenges as the complexity of transactions increases, especially where cross-organizational smart-contract logic and strict endorsement policies are involved (Li et al., 2024). In anti-corruption scenarios, where near-real-time audit trails and competitive bidding workflows are presumed, such limitations will recast integrity choke points from human discretion to system traffic bottlenecks unless architectures and governance policies are designed hand-in-glove. The second is interoperability with legacy systems: government information infrastructures in the U.S. are typically fragmented by program, jurisdiction, and vendor histories. In the absence of shared data standards, identity frameworks, and lifecycle governance, blockchain elements may simply become additional silos and, in fact, integrity layers (Clavin et al., 2020; Clifton, Díaz-Fuentes, & Fernández-Gutiérrez, 2023). Interoperability is meaningful because corruption-resistant procurement oversight relies on linking pre-award, award, contract management, and delivery data across agencies. Interoperability is not optional—it is constitutive of feasibility. Third, sustainability and architecture selection: As in the previous point, while many public-sector proofs of concept reject energy-intensive consensus approaches, feasibility studies still consider efficiency, providing evidence of implementation towards sustainability goals, only here, the design decision to use permissioned or stake-based consensus is as much a policy decision as it is a technical one. (Clifton et al., 2023; Energy Information Administration, 2023).

Institutional capacity is the parallel indicator of feasibility. Training and professionalization will mediate whether blockchain features turn into ongoing anti-corruption controls, or remain as artifacts of the pilot stage. Assistance for the public sector notes the potential for training, professionalization, communities of practice and change-management process, with regard to these features and their use as part of complex socio-technical systems (Dziundziuk & Dziundziuk, 2022). In the U.S., this training and professionalization might also include procurement and records staff who need to realign data stewardship, vendor management, and compliance workflows with new cryptographic and governance primitives. Without such capacity, smart contracts are at risk of being under-defined, and audit trails could risk disconnection from any investigative and oversight functions diluting the H2 indicators even though provided with ostensible technical resources.

Regulatory clarity also scaffolds feasibility. In contrast to civil-law environments with top-down harmonization, the U.S. exhibits a mixture of guidance providing baselines to security and sector specific controls but leaves a chart between enforceability of smart contracts, allocation of data rights across federated actors, and admissibility of audit performance. The National Institute of

Standards and Technology's guidance provides technical baselines (National Institute of Standards and Technology, 2020; Howard & Vachino, 2019), and there have been some interventions in a federal government sandbox-style with respect to piloting different architectures to lessen risk. However, the federal system we can realistically expect to work in means that, in addressing the specificity of governance, there are compromises to be negotiated between layers of various programs (Radonjić, Štaka, & Ivić, 2024). This is not decisive limiting factor: in diffusion in the federal system, enactment can be operationalized with templated policies for distributed technical documents and reference implementations with time-based conditions or warranting agencies who enter into intergovernmental working groups; all of which have relation to institutional isomorphism and patterns of observed digital government reforms (DiMaggio & Powell, 1983; Clifton et al., 2023). In high-risk contexts, the current approaches draw on a general convergence towards permissioned, schemed-based architectures relying heavily on process logging and various forms of selective transparency. In procurement, this typically involves establishing tender issuance, bid submissions, evaluation checkpoints and contract amendments on a tamper-evident ledger, while maintaining secrecy through access controls (or through off-chain protections). The idea was not to approach "blockchain everything," but to create a layer that preserves integrity to meaningfully increase the cost of manipulation, and to layer not a new process but a reduced cost of audit (Ølnes et al., 2017; Clavin et al., 2020). In land records, the prototype designs similarly focused on chain of title provenance and cryptographic anchoring of document hashes and, where discussed as a solution, privacy-preserving claims verification to balancing public discoverability of information with data protection through emerging clause type definitions (Clifton et al., 2023). In both areas, the technology has engaged relatively conservative technical design, meaning they aim to limit novel features to user-facing workflows while concentrating on strengthening some aspects of back-office verifiability. Feasibility is also enhanced by building on complementary analytics. Linking blockchain event streams to anomaly-detection pipelines makes detecting bid-rigging, collusion or other anomalous amendments practically detectable because it creates structured time-sequenced data output for downstream models to utilize (Lakhanpal, Gupta & Singh, 2024). Critically, this is not an argument for algorithmic determinism. It just notes that blockchain's most immediate regulatory anti-corruption value comes when immutable logs provide better quality information to scrutiny and investigative practices already inserted in the state. Aligning the technology's affordances with institutional reality and substantiating H2 without overcommitting to claims of causation.

All mentioned, the U.S. is technically situated for readiness, but contextually contingent. Strong standards and a solid vendor-research system are pragmatic feasibility advantages; while federalism, legacy heterogeneity and uneven capacities are the principal challenges. The diffusion dynamics suggests codified forms will be the vehicles to recast pilots into replicable practices (Rogers, 2003; DiMaggio & Powell, 1983). Comparatively, that now puts the U.S. between slow-moving and more centralized regulatory environments, backed by harmonized provincial systems: the U.S. can move very quickly where there are local champions, the standards align, and the governance options are clear, while it can also stall where all these preconditions are absent

(Clifton et al., 2023; Government of Canada, 2021; European Commission, 2023) . In terms of the implications for this thesis; it is simple to position that H3 stands in as much as the U.S. has a strong technical foundation and milieu to innovate, and its ongoing counteracting corruption impacts are dependent on interoperability governance, skill development initiatives, and policy templates to manage the departments' diverse federalism towards integrity goals.

Lastly, these findings compel the adoption of the context aware implementation path consistent with the thesis framework: (i) a contextual assessment that accounts for legacy interfaces, data custodians, and oversight needs; (ii) design and prototyping that narratively specifies permission Ing, identity, and logging at the granularity of contract or title workflows; (iii) Implementation and scaling with shared schemas and interagency data sharing agreements; and (iv) evaluation and adaptation as audit-relevant measures and post-development learning cycles permit (Clifton et al., 2023; Ølnes et al., 2017). Adopting this implementation path will not promise that corruption will be eliminated, rather it will condition blockchain's technical value on institutional fit, thereby situating the U.S. case with the thesis is overarching comparative insight that technology could be an enabler of integrity, but only to the extent that organizations and rules can take it in.

3.7.4 Comparative Technological Analysis & Implementation Discussion

Blockchain is increasingly studied as a governance technology in public procurement because it offers tamper-resistant records, normalized event logging, and auditable traces of processes. That said, in Italy, Canada, and the United States, the path from testing out pilot projects in experimental settings to integrated and enduring use is subject to digital infrastructure, interoperability with legacy systems, and distinct legal and institutional contexts. A comparative view across the three contexts illustrates shared choices around permissioned or hybrid ledger design; the use of off chain are sensitive data characteristics; and interoperability is as a profile around existing systems of e-procurement, finance and audit. Importantly, the legal environment does more than limit technical choices, it defines them. The following analysis summarizes the state of technological readiness, common challenges, design considerations, and implementation characteristics in each of the three countries, making claims commensurate with what is supported in the cited literature and what we don't know as emerging causal claims (Bouaicha et al., 2024; Cuny, 2022; Zelenski, 2024; Abelseth, 2018; Boysen, 2021; Dziundziuk & Dziundziuk, 2022; Mustafa et al., 2024; Murphy et al., 2021; Howard & Vachino, 2019; Anyanwu et al., 2023; Radonjić et al., 2024; Clavin et al., 2020; Sobolewski & Allessie, 2021; Ba et al., 2023; Wadegaonkar et al., 2024; Sava & Dragos, 2022; Diadia et al., 2022; Fournier & Petrillo, 2018; Lakhanpal et al., 2024; Abdelhamid et al., 2024; Yu et al., 2023; Abdullah et al., 2022; Benítez-Martínez et al., 2022; Baima et al., 2024; Kálmán, 2024; Torkanfar et al., 2023).With relation to pilots in Italy, they have been focused on transparency with respect to procurement, event logging, and contract lifecycle management, and were generally deployed on permissioned platforms to allow role-based access, governance, and integration with administration workflows (e.g., Bouaicha et al., 2024; Cuny, 2021; Torkanfar et al., 2023). These developments occur in the European regulatory environment and the designs fit all of this regional context and consciously and deliberately incorporate the implications of the

GDPR, data minimization, purpose limitation, and erasure rights into the systems. One effect of this is that system architectures, in general, place directly identifiable information off-chain and instead store verifiable commitments (i.e., hashes, timestamps) directly on chain for auditability in a manner which does not effectively store personal data immutably (Kálmán, 2024; Torkanfar et al., 2023). While there certainly are baseline capabilities of national platforms and municipal capabilities, and a good baseline for integration, the fact that there are differences in digital maturity, in addition to variability in legacy systems, means that scaling will need to happen over time and gradually using phased approaches that build progressively from contexts where information and processes are already standardized (i.e., administrative workflows) (Cuny, 2022; Bouaicha et al, 2024; Baima et al., 2024).

Canadian initiatives, like steps or pilots, are also where the aims are largely pilot oriented, such as automating contracts, process automation, breadcrumb traceability, and improved audit trails (Zelenski, 2024; Abelseth, 2018). Urban areas are at the greatest advantage; however, the challenges of interoperating with enterprise-wide procurement suites, along with a convoluted governance structure resulting from the federal–provincial–municipal fragmentation will be significant (Boysen, 2021; Dziundziuk & Dziundziuk, 2022; Murphy et al., 2021). Different privacy obligations, especially those arising from personal information protection regimes, encourage the design of permissioned ledgers that include fine-grained access control measures, sufficient audit logging, and the off-chain storage of sensitive attributes (e.g., Mustafa et al., 2024).As provinces are at different levels of digital capacity and regulatory comfort with digital solutions, adoption plans fit the context better when they support flexible profiles and progressive interoperability rather than all provincial deployments being the same (Murphy et al., 2021; Boysen, 2021).

The US context benefits from a more advanced state of digital and cloud environments, and has seen public-sector pilots in domains related to both procurement and supply chain integrity (Howard & Vachino, 2019; Anyanwu et al., 2023). Still, the federated reality brings diversity to policy, standards, and vendor ecosystems spanning agency boundaries, all of which can complicate interoperation and upscaling (Clavin et al., 2020; Radonjić et al., 2024). US initiatives frequently look to permissioned or consortium designs in order to make different kinds of accountability and access governance possible for separate actors, and rely on phased pilots/scoping on the nature of institutional fit while rolls around legal record status and smart contract enforcement are still emergent (Clavin et al., 2020; Abdullah et al., 2022). The pattern shaping is not a preference for any one blockchain; it is the acknowledgement that identities, access control, and auditability have been best aligned to our current compliance-based context (Howard & Vachino, 2019; Clavin et al., 2020).

Similar technical challenges appear to recur across all three jurisdictions. Firstly, scalability and throughput limitations are especially relevant where procurement workflows generate or trace logs of high-frequency event generation and time-bound actions. While public networks under load and enterprise use cases support permissioned deployments, and in certain circumstances, layer-2 or

sharding-like solutions that can benefit from referencing a larger public chain may offer variable transaction capacity and costs, where governance and security characteristics are consistent (Sobolewski & Allessie, 2021; Ba et al., 2023; Wadegaonkar et al., 2024). In municipal contexts, the constraints of local infrastructure can further exacerbate specific limits and prefer architectures that provide deterministic latency with minimal overhead (Wadegaonkar et al., 2024). Secondly, there is the structural challenge of interoperability with legacy systems. In Italy and Canada, achieving bidirectional interoperability—allowing authoritative records to flow into the ledger and verified state to flow out to e-procurement, ERP and audit tools—is both technically and organizationally difficult (Cuny, 2022; Boysen, 2021; Dziundziuk & Dziundziuk, 2022). The fragmented context of the United States forms an even bigger landscape, potentially increasing paths to integration, and highlights the importance of common profiles or schemas that align for identity, metadata and event semantics (Clavin et al., 2020). Thirdly, public sectors will benefit by exploring the importance of energy and consensus mechanisms choice. Research demonstrates that, for predictable performance, bounded environmental impact, and other pragmatic criteria that are important to government operations, energy-efficient, permissioned consensus (e.g. some versions of proof-of-authority) suits the purposes of public procurement to fit within its operational capacity (Diadia et al., 2022; Fournier & Petrillo, 2018).

The design responses are evident in the literature and coalesce around hybrid architectures that balance upcoming credibility with closure. Sensitive personal data or commercially sensitive data are secured off-chain through existing governance structures; on-chain records establish anchors to event proofs and state transitions allowing for forensic verifications without disclosing protected attributes (Sava & Dragos, 2022; Kálmán 2024, Torkanfar et al., 2023). Where cooperation is needed between multiple ledgers, or in administrative domains, researchers are exploring cross-chain protocols and standards for proofs as mechanisms for approaching collaborative governance, while maintaining source and integrity guarantees (Yu et al., 2023; Clavin et al., 2020). Adjacency with artificial intelligence (AI) and Internet of Things (IoT) is also being studied for strengthening anomaly detection, automating controls, and linking verifiable device attestations with procurement events; each of these incorporations adds to the blockchain's audit layer without impacting its governance assumptions (Lakhanpal et al 2024, Abdelhamid et al., 2024). The one commonality is conservative engineering, reliance, and audibility, rather than the means of open participation per se.

Legal-regulatory environments also directly translate into architectural choices. In Italy, for example, when considering compliance with General Data Protection Regulation (GDPR), participants have forged a unified approach of permission Ing, off-chain management of personally identifiable information and on-chain commitments that provides tamper-evidence while not affecting data subject rights (Kálmán 2024; Torkanfar et al., 2023). In a like manner, Canada’s privacy and data-sovereignty obligations at both federal, and provincial levels have encouraged designs oriented toward restricted participation, role-based permissions, and a clearly delineated separation between verifiable event logs, and protected datasets (Mustafa et al., 2021; Boysen,

2021; Dziundziuk & Dziundziuk, 2022; Murphy, et al., 2021). In the U.S., the motivation for consortium governance, from security available for agencies at state level, and variation between topical state legislations, has encouraged organizations flexible identity frameworks that may be profiled into any requirements of an agency while supporting accountability and continuity of operations, where appropriate pilot-first approaches are available where legal treatment of records, or automation, is not previously determined (Howard & Vachino, 2019; Clavin et al., 2020; Radonjić et al., 2024; Abdullah et al., 2022). Therefore, in all three countries, the relationship between law and technology is not an afterthought, it is the basis on which the ledger's scope, what will be stored and how the ledger systems will interoperate.

Furthermore, implementation is shaped by actor power and institutional inertia. For instance, in Italy, the strong anti-corruption and top-down oversight leverage an impetus for pilots focused on integrity; however, the presence of institutional inertia, gaps in digital skills, and the uneven capacity of regions to support digital initiatives may have de-celebrators within the implementation process (Sava & Dragos, 2022; Bouaicha et al., 2024; Baima et al., 2024). Potential mitigating strategies identified in the literature include training procurement resource people, articulating on-chain responsibilities with off-chain responsibilities clearly, and sequencing deployments based on where there is already structured data with digital workflows (Cuny, 2022; Torkanfar et al., 2023). In Canada, the distribution of authority across federal, provincial, and municipal governance has thwarted adoption to a single trajectory, while the institutional resistance to piloting represents concerns for costs, privacy, and integration risk. Participatory strategies for identifying affected stakeholders early, while also aligning priorities for digitally based governance, appear to be less risky than imposing a mandate (Mustafa et al., 2024; Boysen, 2021; Murphy et al., 2021). Lastly, in the United States, inconsistent vendor ecosystems and varied policy baselines lead to varying degrees of readiness and standards among the governments involved; since pilots can be used to add value in particular workflows, the scaling up depends on collaboration and governance that span agencies and include shared governance of identity, policy, and interoperability (Clavin et al., 2020; Radonjić et al., 2024). In these country contexts, procurement teams are typically focused on operational assurance and auditability; this aligns with ensuring permissioned designs along with energy-sensitive consensus (Fournier & Petrillo, 2018). Based on these findings, there are a number of implementation strategies. Capacity building with respect to procurement, legal, and technical staff reduces resistance created by skillsets, while allowing staff to define detail and articulate requirements; phased implementation that occurs with events, and at the level of (at least) having tamper evident logging of specified process events allows audit evidence, with a defined set of risk management (Cuny, 2022; Sava & Dragos, 2022; Bouaicha et al., 2024). Regulatory sandboxes provide spaces to address compliance behavior, test integration assumptions, and validity performance expectations before deployment (Benítez-Martínez et al., 2022). Standards and profiles for identity, metadata, and event semantics provide a framework for interoperability across agencies and governments; using multiple ledgers does not preclude using cross-chain gateways and patterned proof methods to connect multiple ledgers while managing governance and entrepreneurial integrity (Yu et al., 2023; Clavin et al., 2020). Platform selection

and consensus should primarily consider latency consistency, verifiability, and energy literacy based on contextually suitable public sector operations (Diadia et al., 2022; Fournier & Petrillo, 2018; Ba et al., 2023; Wadegaonkar et al., 2024). Hybrid designs using off-chain storage of sensitive data, while creating on-chain commitments continue to be important products for balancing transparency with privacy and administrative law (Kálmán, 2024; Torkanfar et al., 2023; Sava & Dragos, 2022). Where possible, AI and IoT could enhance anomaly detection and compliance monitoring, so long as models and devices are governance agreements framed with transparency and verification pipelines (Lakhanpal et al., 2024; Abdelhamid et al., 2024).

Cross-jurisdictional learning can be found in drawing attention to where each setting's particular constraints produce transferable patterns. Italy indicated that GDPR aligned permissioned deployments allow verifiable process trails, without permanent immutably-stored personal data (Kálmán, 2024; Torkanfar et al., 2023; Bouaicha et al., 2024). Canada's findings demonstrated the importance of interoperating across federated systems, while also demonstrating practical harmonized profiles that honor privacy obligations, while allowing auditability (Mustafa et al., 2024; Murphy et al., 2024). The US demonstrated that consortium agreements allow autonomous agencies to coordinate while normalizing heterogeneity around shared identity and policy (Clavin et al., 2020; Anyanwu et al., 2023; Radonjić et al., 2024). Importantly, none of these pathways suggest guarantees of corruption reduction; rather they illustrate viable technical and organizational pathways for embedding tamper evident records and automated controls into the procurement lifecycle of an organization consistent with the laws in force and organizational capacity.

In summary, the comparative evidence from Italy, Canada and the US supports one feasible architecture: permissioned (or hybrid) ledgers; data partitioning that preserves privacy; conservative and energy conscious consensus; and, standardized interfaces to legacy systems. Legal regimes shape these choices directly by producing designs that align transparency with privacy and the realities associated with administrative law (Kálmán, 2024; Torkanfar et al., 2023; Mustafa et al., 2024; Clavin et al., 2020). The durability of implementation depends on building capacity, and designing scoped pilots, and interoperability frameworks that allow verification between agencies while respecting local prerogatives. Building capacity, scoped pilots, and, designing interoperability frameworks that allow verification between agencies while respecting local prerogatives. The results of the studies cited so far have been primarily pilot based, but they provide a canvas to review future designs in the literature that illustrate grounded incremental embedding of verifiable tamper evident mechanisms in procurement processes, with a focus on mitigating corruption related risks and strengthening accountability without over-citing evidence effects attributable to the evidence cited.

3.8. Conclusion

3.8.1Summary of Key Findings

This dissertation examined whether, how, and under what institutional conditions blockchain can strengthen integrity in public procurement across Italy, Canada, and the United States. The research design combined a document-based comparative analysis—spanning legal, regulatory, and organizational sources—with a bounded quantitative scaffold of governance indicators (CPI and WGI) that served to contextualize, rather than determine, findings. The analytical strategy mapped procurement lifecycle vulnerabilities to concrete integrity controls and then evaluated the legal predicates and institutional capacities required for those controls to be admissible, governable, and sustainable. This triangulated approach generated convergent evidence across Chapters 4–6 that directly addresses the research questions and permits a systematic revisiting of the study's hypotheses.

First, as to the legal foundations of procurement, the findings demonstrate that feasibility is mediated primarily by the specificity of procurement law, the presence of a coordinating authority, and the evidentiary status of digital records. Italy's "digital-by-default" procurement architecture—anchored in D.Lgs. 36/2023 and implemented through ANAC's governance of the BDNCP and the nationwide publication hub (PCP)—legally mandates certified platforms, structured notices (eForms-IT), and machine-readable publication. These provisions convert transparency from an ex post documentary practice into an ex ante, data-driven legal process, creating a compliant "spine" into which permissioned ledger controls can be credibly integrated. Canada and the United States maintain technology-neutral frameworks but lack procurement-specific accommodation of ledger artefacts: Canada relies on horizontally framed federal policy instruments and federated discretion; the United States retains a records-centric acquisition regime (FAR) without formal recognition of blockchain outputs. Functional admissibility—rather than immutability per se—determines whether ledger records can "count" in audits, disputes, and reviews.

Second, the comparative regulatory landscape coheres around three patterns that explain adoption trajectories. Italy exhibits a codification-led model, in which EU-aligned obligations and ANAC/AgID measures standardize transparency and auditability across the lifecycle. Canada follows a pilot-first model, privileging modular experimentation (e.g., credentialing pilots) without

binding procurement rules that would elevate pilots into an enforceable integrity layer. The United States presents a fragmented model: pilots exist across agencies and states, yet there is no procurement-specific guidance to standardize evidentiary treatment or interoperability. These patterns are not merely descriptive; they explain why similar technical designs travel unevenly across jurisdictions and why empowered intermediaries (regulators, standards bodies, audit authorities) are decisive for institutionalization.

Third, at the procurement lifecycle level, corruption risk is concentrated at repeatable junctions—planning/specifications, bid submission and evaluation, award, implementation, and audit—where permissioned blockchain can function as a verifiable integrity layer. Versioned justifications and role-bound approvals mitigate planning manipulation; hashed and machine-readable notices deter post hoc edits; sealed-bid commitments with threshold opening protect confidentiality while enabling verifiability; deterministic state machines with auditable overrides harden award processes; milestone-gated disbursements tied to attestations constrain delivery fraud; and append-only provenance reduces audit reconstruction risk. The analysis emphasizes human-in-the-loop accountability: smart contracts act as process governors with explicit, identity-bound override steps, preserving reason-giving and review under administrative law.

Fourth, feasibility is not strictly technical. It is socio-legally mediated by identity and access management, cybersecurity baselines, interoperability profiles, and privacy/records doctrines. In Italy, GDPR-compliant architectures require off-chain handling of personal and commercially sensitive data with on-chain proofs, and they foreground role-based authorization and standard interfaces to certified repositories. In Canada, federated pluralism creates privacy-by-design opportunities but introduces variability in retention/admissibility across fora. In the United States, any blockchain-derived artefact must be authenticated and integrated into the legally compiled record to be persuasive. Across all three contexts, identity governance and procurement-grade security determine whether cryptographic assurances translate into institutional trust and enforcement credibility.

Revisiting the hypotheses, the evidence confirms that (H1) legal commonalities and divergences shape adoption; (H2) regulatory logics—codification-led, pilot-first, fragmented—are stable and predictive; (H3) blockchain reduces corruption risks when controls are design-targeted and procedurally embedded (conditional support); (H4) feasibility varies with capacity and is mediated

by organizational and socio-political factors (confirmed); and (H5) cross-jurisdictional learning is feasible only through adaptive transfer of patterns (e.g., off-chain PII/on-chain proofs; audit-grade logging; verifiable credentials), not wholesale transplantation of technologies or clauses. The quantitative scaffold strengthens interpretation by aligning legal–institutional findings with governance trajectories: Italy's recent upward movement in control-of-corruption aligns with the consolidation of digital-by-default procurement; Canada's high but gently declining indicators counsel the conversion of pilots into system standards; and U.S. volatility suggests that technical experimentation without procurement-specific legal adaptation is likely to underperform.

3.8.2. Original Contributions to Knowledge

This dissertation fills a salient research gap at the intersection of blockchain governance and comparative public procurement by developing a multi-level, actor-attentive lens that links lifecycle vulnerabilities, legal predicates, and concrete control designs. Conceptually, it reframes blockchain not as a monolithic "anti-corruption technology" but as a verifiable control architecture whose public value depends on its fit with procurement law, records doctrine, privacy obligations, and organizational governance. The analysis clarifies the conditions under which cryptographic assurances become administratively legible and judicially admissible, thereby moving the field beyond generalized transparency rhetoric toward mechanism–risk fit.

The study theoretically advances socio-technical theories of institutional adoption by elaborating on legal form of procurement (e.g., technology-neutral codes and codified digital-by-default regimes), locus of administrative power (e.g., centralized regulators and federated coordination) and admissibility of machine-readable evidence in conditioning technological affordances. It contributes a comparative typology of regulatory logics—codification-first, pilot-first, fragmented—and demonstrates the role of that logics in contorting the translation of blockchain affordances (immutability, programmability, provenance) into enforceable administrative controls. By incorporating an actor-level analysis—procurement officers, oversight bodies, systems integrators, vendors, suppliers, auditors, and civil society—the dissertation explains why adoption succeeds or stalls in real institutions and how perceived risks are differentially distributed across roles.

Empirically, the dissertation consolidates and interprets comparative data that are typically siloed across legal and technical literatures. It synthesizes the certified platform ecosystem in Italy

(BDNCP/PCP), the policy led pilots and credentialing pathways in Canada, and the fragmented innovation at the United States level with limited adaptation specific to the procurement function. It also places these evidence streams within governance pathways (i.e. CPI and WGI), thus contextualizing procurement-grade blockchain feasibility within larger trends of integrity and capacity. This empirical evidence provides an auditable knowledge base for policy decisions regarding where to place integrity checkpoints and how to phase controls across jurisdictions with varying legal cultures and administrative capacity.

In terms of methodology, the dissertation provides a replicable framework for socio-technical system comparative analysis of government, combining qualitative document analysis with descriptive quantitative indicators while maintaining interpretive rigor. The framework formalizes a "thread map" from risk to control to legal predicate to organizational capacity, enabling cross-jurisdictional comparison without over-claiming causal inference. This approach demonstrates how macro-indicators can discipline interpretation and support transferability diagnostics while respecting the epistemic limits of document-based research. It thus contributes to a maturing methodological toolkit for evaluating complex public-sector technologies where randomized trials are infeasible or ethically constrained.

A further contribution is to the nuanced treatment of blockchain typologies and risks. The study distinguishes permissionless networks from permissioned and consortium models suited to public procurement; clarifies the role of selective anchoring (hashes/timestamps) versus full data replication; and evaluates privacy-preserving patterns (off-chain storage, verifiable credentials, threshold opening, zero-knowledge attestations) as pathways for reconciling immutability with data protection and records law. It surfaces inherent risks—validator concentration and collusion in permissioned settings, key management and identity compromise, mis-specified smart contracts, vendor lock-in through proprietary interfaces, and energy/latency trade-offs—and links each risk to countervailing governance or design controls (e.g., role-based attestations, key escrow with judicial triggers, open interoperability profiles, and lifecycle carbon accounting).

3.8.3. Policy Recommendations

The comparative lessons point to actionable, evidence-based recommendations that respect the principle of adaptive transfer: harmonization does not entail standardization. Instead, jurisdictions should reinterpret portable control patterns in light of national legal traditions, privacy doctrines,

institutional capacities, and political economies. The recommendations below target procurement-grade clarity, interoperability, capacity-building, and risk mitigation, while anticipating actor resistance and incentives.

Italy should convert legal determinacy into operational guidance. Joint ANAC–AgID technical-administrative guidance can codify permissioned-ledger patterns as options within certified platforms—off-chain personal and commercially sensitive data; on-chain proofs and timestamps; role-bound attestations; standardized commit–reveal schemes for sealed bids; and milestone-gated disbursements—while clarifying evidentiary status, retention obligations, and pathways for human-in-the-loop overrides. Aligning node governance with national cybersecurity baselines and adopting open interoperability profiles will reduce vendor lock-in and enable competitive procurement of platform components. Targeted capacity-building for contracting authorities—especially those operating under the qualification regime—should focus on identity lifecycle management, key custody, and audit analytics integrated into the BDNCP/PCP ecosystem.

Canada should bridge pilots to a system-level integrity layer that respects federalism. An intergovernmental framework should authorize the use of permissioned controls for bid commitment, change-order logging, and milestone attestations; standardize evidentiary treatment and retention across forums; and mandate credential and interoperability profiles (e.g., W3C verifiable credentials) for supplier due diligence. Model clauses, procurement playbooks, and audit checklists would lower transaction costs for departments and provinces while preserving autonomy. Regulatory sandboxes should be scoped for procurement-grade features—sealed-bid threshold opening, verifiable milestone payments, and records integration—to accelerate procurement-specific learning rather than general blockchain experimentation.

The United States should promulgate procurement-specific federal guidance. FAR/OFPP interpretive guidance or a Federal Acquisition Circular should clarify how ledger-anchored proofs can be recognized within Parts 4 and 42 (administrative records and contract administration), accompanied by a NIST-aligned interoperability profile and practical records-integration requirements (human-readable exports, authentication chains, cryptographic metadata). Workforce enablement modules through FAI/DAU should cover identity/PKI hygiene, sealed-bid protocols, and audit analytics for blockchain-derived logs. Federal pilots will remain legally

peripheral with no possibility to scale across agencies, in absence of procurement-specific admissibility and interface rules.

While jurisdictions differ, best practices include a larger historical perspective, such as: designing accountability over maximally automating; creating controls at integrity checkpoints where the benefits for verification/obligatory verification are immediate; institutionalizing independent verification and audit analytics; and on the interoperability front, prioritizing open schema, and APIs to decouple cryptographic proofs from application logic. Capacity building should account for roles: procurement officers trained on process and evidentiary implications; Chief Information Security Officers on key management and endpoint security; auditors on analyzing logs; and vendor/suppliers' literacy on credentialing workflows. Risk mitigation should be explicit: countering validator centralization with governance safeguards; in-embedding procedures for override, including reason giving; integrating privacy-preserving proofs; conducting lifecycle energy and cost analysis to avoid sustainability or greenwashing externalities. Influencing actor resistance requires aligning additional incentives - i.e. reducing burdens of audits and payment timeliness - in exchange for compliance with verifiable controls.

3.8.4. Limitations of the Study

The study is intentionally document-based and interpretive. Its quantitative elements are descriptive and used for triangulation; they do not measure corruption reduction causally. Cross-national comparisons abstract from sub-national heterogeneity and variations in administrative culture that may shape implementation and legitimacy. The temporal scope necessarily lags evolving legal doctrines on privacy, records, and digital identity, as well as rapidly changing technical stacks. Actor resistance—stemming from capacity constraints, role redefinition, vendor incentives, or political contestation—could alter feasibility independent of legal or technical design. Finally, procurement-grade performance properties (latency, availability, failure modes) were discussed conceptually rather than measured in live deployments, reflecting the broader empirical gap in the field.

3.8.5. Avenues for Future Research

Future work should pursue longitudinal, multi-site evaluations that pair legal–doctrinal analysis with operational telemetry from deployments at defined integrity checkpoints (notice integrity, sealed-bid opening, change-order logging, milestone payments). Quantitative impact

assessments—using quasi-experimental designs with matched tenders or synthetic controls—could estimate effects on bid competition, price dispersion, delivery timeliness, and dispute incidence. Comparative extensions beyond procurement (e.g., social benefits, licensing, infrastructure monitoring) would test the portability of permissioned control patterns and identify sectoral constraints. Research on blockchain governance should deepen actor-level analysis: validator selection and rotation, key management and recovery with judicial triggers, allocation of decision rights between regulators and platform operators, and legitimacy under administrative law. Privacy-preserving methods warrant rigorous legal–technical evaluation (zk attestations, selective disclosure, revocation), including their auditability and cost profiles. Finally, sustainability assessments should integrate energy, carbon, and cost life-cycle accounting into procurement decisions about digital integrity layers.

3.8.5. Concluding Remarks

The comparative analysis across Italy, Canada, and the United States shows that blockchain's promise in public procurement is real yet conditional. Cryptography does not, by itself, produce integrity; integrity emerges when cryptographic assurances are made legible to law, governed by accountable institutions, and sequenced to existing capacity. Italy demonstrates how codified platform governance creates an ecological niche for permissioned integrity layers; Canada illustrates the potential of pilots that must be translated into admissible, interoperable standards; and the United States highlights the limits of technical experimentation absent procurement-specific legal adaptation. The responsible path forward is calibrated integration: blockchain as a verifiable control architecture that strengthens transparency and accountability while preserving human-in-the-loop discretion. Pursued in this way, blockchain can move from a promising innovation to a durable public integrity infrastructure aligned with the rule-of-law foundations of procurement.

References

A protocol for on-chain tenders. https://doi.org/10.1109/percomworkshops53856.2022.9767325

A systematic literature review: Benefits and challenges of cloud-based big data analytics. Issues in information systems null, https://doi.org/10.48009/1_iis_2023_125

Abdul, M. (2024). Navigating blockchain's twin challenges: Scalability and regulatory compliance. Blockchains, 2, 265–298.

Aburumman, N., Fraij, J., & Szilágyi, R. (2020). Digitalization: The use of blockchain in public sector. *Oradea Journal of Business and Economics*, *5*(2), 72-82.

Adelopo, I., & Rufai, I. (2020). Trust deficit and anti-corruption initiatives. *Journal of Business Ethics*, *163*(3), 429-449.

Adesola, B. M., Kehinde, O., Omonijo, D., Agatha, O. B., Bukar, H. M., Ahmed, A. H., Nuhu, U., & Mudashiru, S. A. (2024). Global corruption: An epidemic beyond national, cultural, religious, job, and ethical boundaries. Cultural Communication and Socialization Journal, 5(2), 54–57. https://doi.org/10.26480/ccsj.02.2024.54.57

Adjorlolo, G., Tang, Z., Wauk, G., Adu Sarfo, P., Braimah, A. B., Blankson Safo, R., & N-yanyi, B. (2025). Evaluating Corruption-Prone Public Procurement Stages for Blockchain Integration Using AHP Approach. *Systems*, *13*(4), 267.

Agenzia per l'Italia Digitale (AgID). (2024). Piano triennale per l'informatica nella Pubblica Amministrazione 2024–2026.

Agenzia per la Cybersicurezza Nazionale (ACN). (2024a). Regolamento cloud per la Pubblica Amministrazione.

Agenzia per la Cybersicurezza Nazionale (ACN). (2024b). Linee guida per il rafforzamento della protezione delle banche dati.

Agwot, K. R. (2024). Exploring Systemic and Behavioral Factors Influencing Corruption in Public Procurement: A Global Comparative Study. Journal of Business and Management Studies, 6(6), 141-149.

Agyeman, A. Y. (2025). Enhancing governance and public sector efficiency through blockchain technology: A simulation study. Asian Journal of Research in Computer Science. https://doi.org/10.9734/ajrcos/2025/v18i3599

Ahmadjonov, M. (2025). The impact of corruption factors in public administration. Review of Law Sciences. https://doi.org/10.51788/tsul.rols.2025.9.1./mmay2885

Ahmed, M. F., Khan, M. R. A. A., Islam, M. R., & Islam, M. N. (2024). AI and Blockchain for Regulatory Compliance: Enhancing Transparency and Efficiency in Governance. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *7*(01), 278-290.

Akanfe, O., Lawong, D., & Rao, H. R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, *76*, 102753.

Akçay, S. (2006). Corruption and human development. *Cato J.*, *26*, 29.

Aliti, A., Leka, E., Luma, A., & Trpkovska, M. A. (2022, May). A Systematic Literature Review on Using Blockchain Technology in Public Administration. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1031-1036). IEEE.

Allessie, D., Sobolewski, M., Vaccari, L., & Pignatelli, F. (2019). Blockchain for digital government. *Luxembourg: Publications Office of the European Union*, 8-10.

Alotaibi, E. M. (2023). A conceptual model of continuous government auditing using blockchain-based smart contracts. *International Journal of Business and Management*, *17*(11), 1-1.

Alves Batista, D. (2024). Enhancing transparency and accountability in public procurement: exploring blockchain technology to mitigate records fraud. *Records Management Journal*, *34*(2/3), 151-170.

American Bar Association. (2000). Model Procurement Code for State and Local Governments.

Anderson, R. D., Jones, A., & Kovacic, W. E. (2024). *Combatting corruption and collusion in public procurement: A challenge for governments worldwide*. Oxford University Press.

Andrade, G. P., Abreu, J. C. A. D., & Santos, R. C. D. (2025). The impact of blockchain on Brazilian public procurement processes from the perspective of transaction costs: scenarios as perceived by experts. *International Journal of Organizational Analysis*, *33*(2), 365-389.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).

Angrist, J. D., & Pischke, J. S. (2009). *Mostly harmless econometrics: An empiricist's companion*. Princeton university press.

Annisa, N. N., & Lavides, M. (2025). The impact of corruption on economic stability and community life in Indonesia. Jurnal Perpajakan dan Keuangan Publik, 4(1). https://doi.org/10.15575/jpkp.v4i1.44798

Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). *Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. Future Internet 2021, 13, 62*.

Anyanwu, A., Dawodu, S. O., Omotosho, A., Akindote, O. J., & Ewuga, S. K. (2023). Review of blockchain technology in government systems: Applications and impacts in the USA. World Journal of Advanced Research and Reviews, 20(3), 863-875.

Anyanwu, A., Dawodu, S. O., Omotosho, A., Akindote, O. J., & Ewuga, S. K. (2023). Review of blockchain technology in government systems: Applications and impacts in the USA. World Journal of Advanced Research and Reviews. https://doi.org/10.30574/wjarr.2023.20.3.2553

Arif, M., Bernard, C., & Philip, L. (2024). Legal implications and challenges of blockchain technology and smart contracts. Computer, 12(2), 2024.

Arrowsmith, S. (2014). The Law of Public and Utilities Procurement (3rd ed.). Sweet & Maxwell.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62.

Autorità Nazionale Anticorruzione (ANAC). (2023a). Delibera n. 261 del 20 giugno 2023 (art. 23 D.Lgs. 36/2023—BDNCP).

Autorità Nazionale Anticorruzione (ANAC). (2023b). Delibera n. 262 del 20 giugno 2023 (art. 24—FVOE).

Autorità Nazionale Anticorruzione (ANAC). (2023c). Delibera n. 263 del 20 giugno 2023 (art. 27—Pubblicità legale).

Autorità Nazionale Anticorruzione (ANAC). (2023d). Delibera n. 264 del 20 giugno 2023 (art. 28—Trasparenza).

Autorità Nazionale Anticorruzione. (2023). Delibera n. 263 del 20 giugno 2023: Disposizioni in materia di pubblicazione legale e trasmissione dati al BDNCP.

Autorità Nazionale Anticorruzione. (2023). Delibera n. 263 del 20 giugno 2023—Provvedimento art. 27 "Pubblicità legale". Gazzetta Ufficiale della Repubblica Italiana, Serie Generale, n. 151 (30/06/2023). https://www.anticorruzione.it/-/delibera-n.-263-del-20-giugno-2023-provvedimento-art.-27-pubblicit%C3%A0-legale

Autorità Nazionale Anticorruzione. (2023). Delibera n. 263/2023—Pubblicità legale. Gazzetta Ufficiale. https://www.anticorruzione.it/-/delibera-n.-263-del-20-giugno-2023-provvedimento-art.-27-pubblicit%C3%A0-legale

Autorità Nazionale Anticorruzione. (2023a). Delibera n. 264 del 20 giugno 2023: Provvedimento attuativo dell'art. 28 del D.Lgs. 36/2023 (Trasparenza dei contratti pubblici). Rome: ANAC.

Autorità Nazionale Anticorruzione. (n.d.). OCDS portal: Public procurement—Italy. https://dati.anticorruzione.it/opendata/ocds_en

Autorité des marchés publics. (2023). Annual report.

Auwal, A. M., & Aminu, S. A. (2020). Blockchain technology: Potentials for public procurement transformation and transparency. International Journal of Public Administration in the Digital Age, 7(2), 45–57. https://doi.org/10.4018/IJPADA.2020040104

Avdasheva, S., Korneeva, D., & Yusupova, G. (2025). Artificial intelligence against collusion: What (not) to expect? Voprosy Ekonomiki, 2025(4), 34–54. https://doi.org/10.32609/0042-8736-2025-4-34-54

Ba, P. D., Tamgno, J. K., & Kora, A. D. (2022). Dematerialization of public procurement approach based on Hyperledger Fabric blockchain using OCDS. In 2022 IEEE International Conference on e-Business Engineering (ICEBE) (pp. 184–189). IEEE.

Diadia, P., Tamgno, J. K., & Kora, A. D. (2023, October). Implementing and evaluating a blockchain-based dematerialized public procurement system with hyperledger fabric and ocds. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA)* (pp. 136-141). IEEE.

Bai, Y., Hu, Q., Seo, S. H., Kang, K., & Lee, J. J. (2021). Public participation consortium blockchain for smart city governance. *IEEE Internet of Things Journal*, *9*(3), 2094-2108.

Bai, Y., Liu, L., Li, W., & Yu, Y. (2022). Evaluating blockchain adoption in government procurement: A stakeholder perspective. Government Information Quarterly, 39(2), 101700. https://doi.org/10.1016/j.giq.2021.101700

Bălan-Liseanu, R.-C. (2023). Corruption—Global threat to human security. International Conference Knowledge-Based Organization, 29(1), 9–16. https://doi.org/10.2478/kbo-2023-0029

Bank Secrecy Act, 31 U.S.C. 5311–5330.

Baranwal, P. R. (2020). Blockchain-based full privacy-preserving public procurement [Preprint].

Barbereau, T. J., & Bodó, B. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. Computer Law & Security Review, 49, 105829. https://doi.org/10.1016/j.clsr.2023.105829

Basdevant, O., Abdou, A., Fazekas, M., & Dávid-Barrett, E. (2022). Assessing vulnerabilities to corruption in public procurement and their price impact. IMF Working Papers, 2022(103). https://doi.org/10.5089/9798400207884.001

Basheka, B. (2021). Public procurement governance: Toward an anti-corruption framework for public procurement in Uganda. In Public Procurement, Corruption and the Crisis of Governance in Africa (pp. 113–141). Springer. https://doi.org/10.1007/978-3-030-63857-3_7

Batista, D. A. (2024). Enhancing transparency and accountability in public procurement: Exploring blockchain technology to mitigate records fraud. Records Management Journal, 34(2), 151–170. doi:10.1108/RMJ-10-2023-0054

Batory, A. (2012). Why do anti-corruption laws fail in Central Eastern Europe? A target compliance perspective. Regulation & Governance, 6(1), 66–82. https://doi.org/10.1111/j.1748-5991.2011.01125.x

Batubara, F., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. Proceedings of the 19th Annual International Conference on Digital Government Research. https://doi.org/10.1145/3209281.3209317

Batubara, F., Ubacht, J., & Janssen, M. (2019). Unraveling transparency and accountability in blockchain. Proceedings of the 20th Annual International Conference on Digital Government Research. https://doi.org/10.1145/3325112.3325262

Bauhr, M., Czibik, Á., de Fine Licht, J., & Fazekas, M. (2020). Lights on the shadows of public procurement: Transparency as an antidote to corruption. Governance, 33(3), 495–523. https://doi.org/10.1111/gove.12432

Benítez-Martínez, F. L., Romero-Frías, E., & Hurtado-Torres, M. (2022). Neural blockchain technology for a new anticorruption token: Towards a novel governance model. Journal of Information Technology & Politics, 20, 1–18. https://doi.org/10.1080/19331681.2022.2027317

Bennett, L. (2024). The Role of Blockchain Technology in Enhancing Supply Chain Transparency in Italy.

Berberich, M., & Steiner, M. (2016). Blockchain technology and the GDPR – How to reconcile privacy and distributed ledgers? European Data Protection Law Review, 2(3), 422–426. https://doi.org/10.21552/EDPL/2016/3/21

Berman, P. S. (2007). Global legal pluralism. Southern California Law Review, 80(5), 1155–1238.

Bernabe, J. B., Cánovas, J. L., Hernández-Ramos, J., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872

Bhagat, G., & Jha, K. (2023). Corruption risks in public construction. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction. https://doi.org/10.1061/jladah.ladr-936

Bhutta, M. N. M., Khwaja, A., Nadeem, A., Ahmad, H., Khan, M., Hanif, M., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. IEEE Access, 9, 61048–61073. https://doi.org/10.1109/ACCESS.2021.3072849

Blemus, S. (2018). Law and blockchain: A legal perspective on current regulatory trends worldwide. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3080639

Blue & Gold Fleet, L.P. v. United States, 492 F.3d 1308 (Fed. Cir. 2007).

Bodó, B., & Janssen, H. (2022). Maintaining trust in a technologized public sector. Policy and Society. https://doi.org/10.1093/polsoc/puac019

Bokolo Anthony Jr. (2023). Deployment of distributed ledger and decentralized technology for transition to smart industries. Environment Systems and Decisions, 43, 298–319.

Bolívar, M. P. R., & Prados, M. J. R. (2022). Blockchain for open government: The case of public procurement. Government Information Quarterly, 39(3), 101713. https://doi.org/10.1016/j.giq.2022.101713

Bollen, K. A. (1989). Structural equations with latent variables. Wiley.

Bouaicha, M. A., Montanaro, T., Lasla, N., Vergine, V., Sergi, I., & Patrono, L. (2024, June). A Blockchain-Based System with Anomaly Exclusion Method to Enhance Transparency and Fairness in Italian Public Procurement. In *2024 9th International Conference on Smart and Sustainable Technologies (SpliTech)* (pp. 1-6). IEEE.

Löffler, E. (2003). *Public management and governance*. Routledge.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3), 187-223.

Brinkmann, M. (2021). The realities of blockchain-based new public governance. Digital Government: Research and Practice, 2, 1–14. https://doi.org/10.1145/3462332

Brownsword, R., & Goodwin, M. (2012). Law and the Technologies of the Twenty-First Century. Cambridge University Press.

Bustamante, P., et al. (2022). Government by code? Blockchain applications to the public sector. Frontiers in Blockchain, 5, 869665. doi:10.3389/fbloc.2022.869665

Cagigas, D., Clifton, J., Díaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for public services: A systematic literature review. IEEE Access, 9, 13904–13921. https://doi.org/10.1109/ACCESS.2021.3052019

Cagigas, D., Clifton, J., Diaz-Fuentes, D., Fernández-Gutiérrez, M., & Harpes, C. (2023). Blockchain in government: toward an evaluation framework. *Policy Design and Practice*, *6*(4), 397-414.

Cal. Pub. Contract Code.

Canada (Minister of Citizenship and Immigration) v. Vavilov, 2019 SCC 65.

Canada Evidence Act, R.S.C. 1985, c. C-5.

Canadian Free Trade Agreement (CFTA). (2017). Agreement on internal trade: Procurement chapter and annexes.

Canadian Free Trade Agreement Secretariat. (2017). Canadian Free Trade Agreement, Chapter Five: Government Procurement.

Canadian International Trade Tribunal. (2023). Procurement inquiries: Practice and procedures.

Cappai, M. (2023). The role of private and public regulation in the case study of crypto-assets: The Italian move towards participatory regulation. Computer Law & Security Review, 49, 105831. https://doi.org/10.1016/j.clsr.2023.105831

Carvalho, A. (2019). Digital public governance and blockchain technologies: A legal perspective from Italy. In Blockchain and Public Administration (pp. 117–138). Springer.

Casado Vara, R., Prieto, J., De la Prieta, F., & Corchado, J. M. (2021). Blockchain framework for IoT data protection in smart cities. Sensors, 21(4), 1282. https://doi.org/10.3390/s21041282

Čeke, B., Vujović, A., & Banjanović-Mehmedović, L. (2022). Smart contract-based system for public procurement process. In 2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1–5). IEEE. https://doi.org/10.1109/INFOTEH54755.2022.9786157

Čeke, D., Buzadija, N., & Kunosić, S. (2022, March). Enhancing transparency and fairness in public procurement process with the support of blockchain technology: a smart contract based approach. In 2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-6). IEEE.

Čeke, D., Buzađija, N., & Kunošić, S. (2022, March). Enhancing transparency and fairness in public procurement with blockchain: A smart contract–based approach. In 2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH). IEEE.

Centech Group, Inc. v. United States, 554 F.3d 1029 (Fed. Cir. 2009).

Centobelli, P., Cerchione, R., Esposito, E., & Oropallo, E. (2021). Surfing blockchain wave, or drowning? Shaping the future of distributed ledgers and decentralized technologies. Technological Forecasting and Social Change, 165, 120463. https://doi.org/10.1016/j.techfore.2020.120463

Chabrost, M. (2020). Challenges in public procurement. In M. Trybus & R. Caranta (Eds.), Public Procurement Regulation in (a) Crisis? (pp. 129–147). Routledge. https://doi.org/10.4324/9781003023470-11

Chadaeva, T. (2024). U.S. approaches to regulating digital assets. USA & Canada: Economics – Politics – Culture. https://doi.org/10.31857/s2686673024040062

Chiappinelli, O. (2016). Political corruption in the execution of public contracts. Microeconomics: Asymmetric & Private Information eJournal. https://doi.org/10.2139/ssrn.2838638

Chowdhury, M., Ferdous, M., Biswas, K., Chowdhury, N., Kayes, A., Alazab, M., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. IEEE Access, 7, 167930–167943. https://doi.org/10.1109/ACCESS.2019.2953729

Chu, H., Zhang, P., Dong, H., Xiao, Y., Ji, S., & Li, W. (2023). A Survey on Smart Contract Vulnerabilities: Data Sources, Detection and Repair. Information and Software Technology. https://doi.org/10.1016/j.infsof.2023.107282

City of Vienna. (2022). Open Government Data (OGD) – Change Protocol and Notarization. Digitales Wien. Retrieved from https://digitales.wien.gv.at/en/open-government-in-vienna/

Civil Practice Law and Rules, N.Y. C.P.L.R. art. 78.

Clark, R., Coviello, D., Gauthier, J., & Shneyerov, A. (2018). Bid rigging and entry deterrence in public procurement: Evidence from an investigation into collusion and corruption in Quebec. The Journal of Law, Economics, and Organization, 34(4), 491–531. https://doi.org/10.1093/jleo/ewy011

Commodity Exchange Act, 7 U.S.C. §§ 1–27f.

Competition in Contracting Act, 41 U.S.C. 3301.

Constitution Act, 1867 (UK), 30 & 31 Vict., c. 3 (reprinted in RSC 1985, App II, No. 5).

Contract Disputes Act, 41 U.S.C. 7101–7109.

Corte di giustizia dell'Unione europea. (2019). Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), C-507/17.

Corte di giustizia dell'Unione europea. (2022). TU, RE v. Google LLC, C-460/20.

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ("EPPO"). Official Journal of the European Union, L 283, 1–71.

Curry, D. (2024). Limitations of trust and legitimacy in blockchain: Exploring the effectiveness of decentralisation, immutability and consensus mechanisms in blockchain governance. International Journal of Public Sector Management. https://doi.org/10.1108/ijpsm-12-2023-0368

Darabad, B. G., & Dadgar, B. (2017). Public procurement: A major potential for corruption. Global Journal of Politics and Law Research, 4(2), 93–96. https://consensus.app/papers/public-procurement-a-major-potential-for-corruption-dadgar-darabad/88cbda4815815e65a4751efca2abec3a/

Dávid-Barrett, E. (2023). State capture and development: A conceptual framework. Journal of International Relations and Development, 26(2), 224–244.

Dávid-Barrett, E., & Fazekas, M. (2020). Anti-corruption in aid-funded procurement: Is corruption reduced or merely displaced? World Development, 132, 105000. https://doi.org/10.1016/j.worlddev.2020.105000

Dávid-Barrett, E., & Fazekas, M. (2020). Grand corruption and government change: An analysis of partisan favoritism in public procurement. European Journal on Criminal Policy and Research, 25(4), 397–417. https://doi.org/10.1007/s10610-019-09416-4

De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.

Debarment and Suspension (Nonprocurement), 2 C.F.R. pt. 180.

Decarolis, F., & Giorgiantonio, C. (2020). Corruption red flags in public procurement: New evidence from Italian calls for tenders. EPJ Data Science, 11, Article 39. https://doi.org/10.1140/epjds/s13688-022-00325-x

Decreto legislativo 31 marzo 2023, n. 36 (Codice dei contratti pubblici).

Decreto legislativo 31 marzo 2023, n. 36. Codice dei contratti pubblici (Italy).

Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. ch. 2.

Demeshko, A., Astbury, C. C., Lee, K., Clarke, J., Cullerton, K., & Penney, T. (2024). The role of corruption in global food systems: A systematic scoping review. Globalization and Health, 20, Article 31. https://doi.org/10.1186/s12992-024-01054-8

DFARS 252.204-7012; DFARS 252.204-7019; DFARS 252.204-7020; DFARS 252.204-7021.

Diadia, P., Tamgno, J. K., & Kora, A. D. (2022, October). Dematerialization of public procurement based on Hyperledger Fabric using OCDS. In 2022 IEEE International Conference on E-Business Engineering (ICEBE). IEEE.

Diadia, P., Tamgno, J. K., & Kora, A. D. (2022, October). Dematerialization of public procurement approach based on hyperledger fabric blockchain using OCDS. In 2022 IEEE International Conference on e-Business Engineering (ICEBE) (pp. 184-189). IEEE.

Digital Accountability and Transparency Act of 2014, Pub. L. No. 113-101.

Digital ID & Authentication Council of Canada. (2022). Pan-Canadian Trust Framework (PCTF): Overview.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.

Dimant, E., & Tosato, G. (2018). Causes and effects of corruption: What has past decade's empirical research taught us? A survey. Journal of Economic Surveys, 32(2), 335–377. https://doi.org/10.1111/joes.12198

Dincer, O., & Johnston, M. (2025). Corruption in America. Cambridge University Press. https://doi.org/10.1017/9781009423380

Dinde, S., & Shirgave, S. (2023, January). Improved food traceability for restaurant customers using blockchain technology. In 2023 International Conference for Advancement in Technology (ICONAT) (pp. 1–7). IEEE.

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. Official Journal of the European Union, L 305, 17–56.

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. Official Journal of the European Union, L 94, 65–242.

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement. Official Journal of the European Union, L 94, 65–242.

Doguchaeva, S., Zubkova, S., & Katrashova, Y. (2022). Blockchain in public supply chain management: advantages and risks. Transportation Research Procedia, 63, 2172-2178.

Dolowitz, D., & Marsh, D. (2000). Learning from abroad: The role of policy transfer in contemporary policy-making. Governance, 13(1), 5–24.

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. PeerJ Computer Science, 9, e1705. https://doi.org/10.7717/peerj-cs.1705

Double N Earthmovers Ltd. v. Edmonton (City), 2007 SCC 3.

Dubey, S., Singh, P., Verma, R. K., & Kamboj, D. (2023, June). Government tender allocation using blockchain technology. In 2023 international conference on IoT, communication and automation technology (ICICAT) (pp. 1-6). IEEE.

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. International Journal, 72(4), 538–562. https://doi.org/10.1177/0020702017741909

Dutta, R., Das, A., Dey, A., & Bhattacharya, S. (2020). Blockchain vs GDPR in collaborative data governance. In Collaborative Computing: Networking, Applications and Worksharing (pp. 81–92). https://doi.org/10.1007/978-3-030-60816-3_10

Dziundziuk, B., & Dziundziuk, V. (2022). Problems and opportunities of blockchain technologies implementation in public authorities. Journal of Public Administration, 2. https://doi.org/10.26565/1727-6667-2022-2-01

Dziundziuk, B., & Dziundziuk, V. (2025). Methodology for integrating blockchain into digital governance systems: Analysis of challenges, benefits, and opportunities for society. Science and Public Policy. https://doi.org/10.1093/scipol/scaf022

Dziundziuk, V., & Dziundziuk, B. (2022). Implementation of Management Decisions for the Implementation of Blockchain Technologies in Public Authorities. Theory and practice of public administration, 1(74), 7-21.

Dziundziuk, V., & Dziundziuk, B. (2022). Public administration using blockchain technology and platforms: new opportunities. Pressing Problems of Public Administration, 2(61), 104-115.

Dziundziuk, V., & Dziundziuk, B. (2022a). Problems and opportunities of blockchain technologies implementation in public authorities. https://doi.org/10.26565/1727-6667-2022-2-01

Dziundziuk, V., & Dziundziuk, B. (2022b). Public administration using blockchain technology and platforms: New opportunities. https://doi.org/10.26565/1684-8489-2022-2-07

Electronic Commerce Act, 2000, S.O. 2000, c. 17.

Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001–7031.

Electronic signatures; validity of electronic records and signatures, 15 U.S.C. 7001–7031.

Elliott, K. A. (1998). Corruption and the global economy. Foreign Affairs, 77(3), 134–138. https://doi.org/10.2307/20048900

Ellul, J., Galea, J., Ganado, M., McCarthy, S., & Pace, G. (2020). Regulating blockchain, DLT and smart contracts: A technology regulator's perspective. ERA Forum, 21(2), 209–220. https://doi.org/10.1007/s12027-020-00617-7

Enste, D., & Heldman, C. (2018). The consequences of corruption: What do we know from the literature? Edward Elgar. https://doi.org/10.4337/9781786434753.00011

Esposito, M., Tse, T., & Goh, D. (2025). Decentralizing governance: Exploring the dynamics and challenges of digital commons and DAOs. Frontiers in Blockchain. https://doi.org/10.3389/fbloc.2025.1538227

European Commission. (2021). European Blockchain Services Infrastructure (EBSI). Retrieved fromhttps://ec.europa.eu/digital-strategy/our-policies/european-blockchain-services-infrastructure-ebsi_en

European Parliament, & Council of the European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union, L 257, 73–114. https://eur-lex.europa.eu/eli/reg/2014/910/oj

European Parliament, & Council of the European Union. (2014). Regulation (EU) No 910/2014 (eIDAS). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2014/910/oj

European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament, & Council of the European Union. (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, L, 22 December 2023. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

European Parliament, & Council of the European Union. (2023). Regulation (EU) 2023/2854 (Data Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

European Union. (2014). Directive 2014/24/EU of the European Parliament and of the Council, Article 22.

European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 16–17.

European Union. (2019). Implementing Regulation (EU) 2019/1780 (eForms).

European Union. (2022). Regulation (EU) 2022/858 (DLT Pilot Regime).

European Union. (2024). Regulation (EU) 2024/1183 (eIDAS 2.0).

Executive Order No. 12,549, 51 Fed. Reg. 6370 (Feb. 18, 1986).

Executive Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

Fairness in Italian Public Procurement. In 2024 9th International Conference on Smart and Sustainable Technologies (SpliTech) (pp. 1-6). IEEE.

Falcón-Cortés, A., Aldana, A., & Larralde, H. (2021). Practices of public procurement and the risk of corrupt behavior before and after the government transition in México. EPJ Data Science, 10(27), 1–26. https://doi.org/10.1140/epjds/s13688-022-00329-7

Falcón-Cortés, A., Aldana, A., & Larralde, H. (2022). Practices of public procurement and the risk of corrupt behavior before and after the government transition in México. EPJ Data Science, 11, Article 29. https://doi.org/10.1140/epjds/s13688-022-00329-7

False Claims Act, 31 U.S.C. 3729–3733.

Faria, I. (2023). Blockchain in the EU: Transforming imaginaries and the social making of financial regulation. Anthropology Today, 39(3), 15–19. https://doi.org/10.1111/1467-8322.12829

Fauziah, A. Y., & Marpaung, J. (2024). Conflict of interest in public procurement. JIMEK: Jurnal Ilmiah Mahasiswa Ekonomi, 7(1), 1–12. https://doi.org/10.30737/jimek.v7i1.5638

Fazekas, M., & Kocsis, G. (2017). Uncovering high-level corruption: Cross-national objective corruption risk indicators using public procurement data. British Journal of Political Science, 50(1), 155–164. https://doi.org/10.1017/S0007123417000461

Fazekas, M., & Kocsis, G. (2020). Uncovering high-level corruption: Cross-national objective corruption risk indicators using public procurement data. British Journal of Political Science, 50(1), 155–164. https://doi.org/10.1017/S0007123417000461

Fazekas, M., & Tóth, I. (2016). From corruption to state capture: A new analytical framework with empirical applications from Hungary. Political Research Quarterly, 69(2), 320–334. https://doi.org/10.1177/1065912916639137

Fazekas, M., & Wachs, J. (2020). Corruption and the network structure of public contracting markets across government change. Politics and Governance, 8(2), 153–166. https://doi.org/10.17645/pag.v8i2.2707

Fazekas, M., Cingolani, L., & Tóth, B. (2016). A comprehensive review of objective corruption proxies in public procurement: Risky actors, transactions, and vehicles of rent extraction. Social Science Research Network (SSRN). https://doi.org/10.2139/ssrn.2891017

Fazekas, M., Sberna, S., & Vannucci, A. (2021). The extra-legal governance of corruption: Tracing the organization of corruption in public procurement. Governance, 34(3), 569–588. https://doi.org/10.1111/gove.12648

Fazekas, M., Tóth, I. J., & King, L. P. (2016). An objective corruption risk index using public procurement data. European Journal on Criminal Policy and Research, 22(3), 369–397. https://doi.org/10.1007/s10610-016-9308-z

Fazekas, M., Tóth, I. J., & King, P. L. (2016). An objective corruption risk index using public procurement data. European Journal on Criminal Policy and Research, 22(3), 369–397.

Federal Acquisition Regulation (FAR), 48 C.F.R. ch. 1.

Federal Acquisition Regulation (FAR), 48 C.F.R. ch. 1.

Federal Acquisition Regulation, 48 C.F.R. ch. 1 (including FAR subpart 4.5; FAR 4.8; FAR 15.506; FAR 52.243-1).

Federal Acquisition Regulation, Subpart 4.5—Electronic commerce in contracting (United States).

Federal Awardee Performance and Integrity Information System, 41 U.S.C. 2313.

Federal Information Security Modernization Act, 44 U.S.C. 3551–3558.

Federal Records Act (records management), 44 U.S.C. chs. 31, 33; 36 C.F.R. pts. 1220–1239.

Federal Records Act, 44 U.S.C. chs. 31 and 33.

Federal Rules of Evidence (United States Courts). (2023).

Federal supply schedules; use by other entities, 40 U.S.C. 502.

FedRAMP Authorization Act, Pub. L. No. 117-263 (2022).

Feikema, L. T. (2024). Anti-corruption law as a fiction: The illusion of serving morality by controlling it through rules and regulations with an international reach. Global Perspectives, 4(1), 115472. https://doi.org/10.1525/gp.2024.115472

Ferwerda, J., Deleanu, I., & Unger, B. (2016). Corruption in public procurement: Finding the right indicators. European Journal on Criminal Policy and Research, 23(2), 245–267. https://doi.org/10.1007/s10610-016-9312-3

Ferwerda, J., Deleanu, I., & Unger, B. (2016). Corruption in public procurement: Finding the right indicators. European Journal on Criminal Policy and Research, 23(2), 245–267. https://doi.org/10.1007/s10610-016-9312-3

Ferwerda, J., Deleanu, I., & Unger, B. (2017). Corruption in public procurement: Finding the right indicators. European Journal on Criminal Policy and Research, 23(2), 245–267.

Financial Administration Act, R.S.C., 1985, c. F-11.

Finck, M. (2019). Blockchain Regulation and Governance in Europe. Cambridge University Press.

Fonderico, G. (2024). Transparency and Corruption Prevention in the New Public Procurement Code. STUDIES AND RESEARCH .

Franzoni, S. F. S. (2025). Quantifying corruption: The urgent need for metrics. Statistical Journal of the IAOS, 41(2), 233–248. https://doi.org/10.1177/18747655251333097

Freedom of Information Act, 5 U.S.C. § 552 (United States).

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31.

Frizzo-Barker, J., Chow-White, P., Adams, P., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. International Journal of Information Management, 51, 102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014

Gallego, J., Rivero, G., & Martinez, J. (2020). Preventing rather than punishing: An early warning model of malfeasance in public procurement. International Journal of Forecasting, 37(1), 360–377. https://doi.org/10.1016/j.ijforecast.2020.06.006

Galli, E., Martini, M., & Rossi, A. (2023). Digital transformation in Italian public administration: Barriers and lessons for future reforms. Public Policy and Administration, 38(2), 239–256.

GAO (Government Accountability Office). (2023). Blockchain Technology in Federal Agencies: Status and Challenges. GAO-23-104567. Retrieved from https://www.gao.gov/products/gao-23-104567

GAO Bid Protest Regulations, 4 C.F.R. pt. 21.

Gara, M., Iezzi, S., & Siino, M. (2024). Corruption risk indicators in public procurement: A proposal using Italian open data (Quaderni dell'antiriciclaggio No. 23). Unità di Informazione Finanziaria per l'Italia (Banca d'Italia).

García, A. S. (2019). La planificación de los contratos públicos como posible fuente de transparencia administrativa. Revista española de la transparencia, (8), 101-119.

Garcia, P. (2019). Corruption in global health: The open secret. The Lancet, 394(10214), 2119–2124. https://doi.org/10.1016/s0140-6736(19)32527-9

General Services Administration Acquisition Manual (GSAM), 48 C.F.R. ch. 5.

General Services Administration. (n.d.-a). Login.gov: Identity verification (IAL2).

General Services Administration. (n.d.-b). SAM.gov: Contract Opportunities.

Gietzmann, M., & Grossetti, F. (2021). Blockchain and other Distributed Ledger Technologies: Where is the Accounting? SSRN. https://ssrn.com/abstract=3507602

Gillespie, J. (2021). Developing a public interest response to state-orchestrated corruption. Law & Social Inquiry, 47(1), 25–54. https://doi.org/10.1017/lsi.2021.4

Global Affairs Canada. (2023). Government procurement obligations under Canada's trade agreements.

Gnaldi, M., & del Sarto, S. (2024). Measuring corruption risk in public procurement over emergency periods. Social Indicators Research, 170, 445–475. https://doi.org/10.1007/s11205-024-03331-w

Gola, C., Cappa, V., Fiorenza, P., Granata, P., Laurino, F., Lesina, L., ... & Marcelli, G. (2023). La governance delle blockchain e di sistemi basati sulla tecnologia dei registri distribuiti (The Governance of Blockchains and System Based on Distributed Ledger Technology). Bank of Italy Occasional Paper, (773).

Gong, T., Tao, X., Das, M., Liua, Y., & Chenga, J. (2022). Blockchain-based E-tendering evaluation framework. International Journal of Automation & Digital Transformation, 1(1), 75-93.

Government Accountability Office bid protest jurisdiction, 31 U.S.C. 3551–3556; automatic stay, 31 U.S.C. 3553.

Government Contracts Regulations, SOR/87-401.

Government of Canada, Treasury Board Secretariat. (2023). Guideline on multi-factor authentication.

Government of Canada, Treasury Board Secretariat. (n.d.). GCKey: Sign-in and registration.

Government of Canada. (1985). Access to Information Act, R.S.C., 1985, c. A-1.

Government of Canada. (1985). Canada Evidence Act, R.S.C., 1985, c. C-5.

Government of Canada. (1985/2024). Canada Evidence Act, R.S.C., 1985, c. C-5 (ss. 31.1–31.8). https://laws-lois.justice.gc.ca/eng/acts/c-5/

Government of Canada. (1985/2024). Canada Evidence Act, R.S.C., 1985, c. C-5. https://laws-lois.justice.gc.ca/eng/acts/c-5/

Government of Canada. (1985/2025). Access to Information Act, R.S.C., 1985, c. A-1. https://laws-lois.justice.gc.ca/eng/acts/a-1/

Government of Canada. (1985/2025). Access to Information Act, R.S.C., 1985, c. A-1. https://laws-lois.justice.gc.ca/eng/acts/a-1/

Government of Canada. (2000). Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Government of Canada. (2000). Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

Government of Canada. (2000). Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

Government of Canada. (2005). Secure Electronic Signature Regulations, SOR/2005-30. https://laws-lois.justice.gc.ca/eng/regulations/sor-2005-30/

Government of Canada. (2005). Secure Electronic Signature Regulations, SOR/2005-30. https://laws-lois.justice.gc.ca/eng/regulations/sor-2005-30/

Government of Canada. (2018, August 22). Government of Canada exploring the potential of blockchain technology [Press release]. Retrieved from https://www.newswire.ca/news-releases/government-of-canada-exploring-the-potential-of-blockchain-technology-670113383.html

Government of Canada. (2023). Innovation in Public Sector Digital Services. Treasury Board Secretariat. Retrieved from https://www.canada.ca/en/government/digital-services.html

Governo della Repubblica Italiana. (2023). Decreto legislativo 31 marzo 2023, n. 36—Codice dei contratti pubblici. Gazzetta Ufficiale della Repubblica Italiana, Serie Generale, n. 77 (Suppl. Ord. n. 12). https://www.gazzettaufficiale.it/eli/id/2023/04/13/23A02179/sg

Governo della Repubblica Italiana. (2023). Decreto legislativo 31 marzo 2023, n. 36—Codice dei contratti pubblici. Gazzetta Ufficiale. https://www.gazzettaufficiale.it/eli/id/2023/04/13/23A02179/sg

Govindan, K., Jain, P., Singh, R. K., & Mishra, R. (2024). Blockchain technology as a strategic weapon to bring procurement 4.0 truly alive: Literature review and future research agenda. Transportation Research Part E: Logistics and Transportation Review, 181, 103352.

Gow, G. A., & Paré, D. J. (2021). Digital identity policy in Canada: A layered and networked approach. Canadian Journal of Communication, 46(2), 295–316.

Grandes, M., & Coremberg, A. (2020). Corruption accounting and growth: Towards a new methodology. Journal of Financial Crime, 27(1), 43–57. https://doi.org/10.1108/jfc-04-2019-0039

Gray, N. (2021). When anti-corruption fails: The dynamics of procurement in contemporary South Africa. Review of African Political Economy, 48(169), 369–384. https://doi.org/10.1080/03056244.2021.1932789

Gray, N. (2021). When anti-corruption fails: The dynamics of procurement in contemporary South Africa. Review of African Political Economy, 48(169), 369–384. https://doi.org/10.1080/03056244.2021.1932789

Graycar, A. (2015). Corruption: Classification and analysis. Policy and Society, 34(2), 87–96.

Graycar, A. (2015). Corruption: Classification and analysis. Policy and Society, 34(2), 87–96. https://doi.org/10.1016/j.polsoc.2015.04.001

Graycar, A. (2019). Mapping corruption in procurement. Journal of Financial Crime, 26(3), 723–729. https://doi.org/10.1108/JFC-06-2018-0063

Graycar, A. (2022). Corrupt procurement: Rethinking the roles of principals and agents. Policy Design and Practice, 5(3), 276–293. https://doi.org/10.1080/25741292.2022.2113461

Graycar, A., & Sidebottom, A. (2012). Corruption and control: A corruption reduction approach. Journal of Financial Crime, 19(4), 384–399. https://doi.org/10.1108/13590791211266377

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3, 100067. https://doi.org/10.1016/j.bcra.2022.100067

Gyimah-Brempong, K. (2002). Corruption, economic growth, and income inequality in Africa. Economics of Governance, 3(3), 183–209. https://doi.org/10.1007/s101010200045

Habiburrochman, H., Saa, S., Indrayana, D., Khairunnisah, K., & Rahma, F. (2024). Tackling corruption in the public sector: Innovative approaches and policy reforms. Deleted Journal, 1 (6), . https://doi.org/10.59613/ejan4589

Haffar, S., & Özceylan, E. (2024). Blockchain-based system for supplier selection in sustainable and leagile supply chains. IEEE Access.

Hafid, A., Hafid, A., & Samih, M. (2020). Scaling blockchains: A comprehensive survey. IEEE Access, 8, 125244–125262. https://doi.org/10.1109/ACCESS.2020.3007251

Hajnal, Á. (2025). Rational autocrats? Drivers of corruption patterns in competitive authoritarian regimes: Towards an explanatory framework with empirical applications from Hungary. European Political Science, 24, 178–197.

Heeks, R., & Mathisen, H. (2012). Understanding success and failure of anti-corruption initiatives. Crime, Law and Social Change, 58(5), 533–549. https://doi.org/10.1007/s10611-011-9361-y

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. Law, Innovation and Technology, 12(2), 156–174. https://doi.org/10.1080/17579961.2020.1727094

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain-based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Heywood, P., & Rose, J. (2014). "Close but no cigar": The measurement of corruption. Journal of Public Policy, 34(3), 507–529. https://doi.org/10.1017/S0143814X14000099

Hudon, P.-A., & Garzón, C. (2016). Corruption in public procurement: Entrepreneurial coalition building. Crime, Law and Social Change, 66(3), 291–311. https://doi.org/10.1007/s10611-016-9628-4

Ibáñez, L., O'Hara, K., & Simperl, E. (2018). Blockchains and the General Data Protection Regulation. In Blockchain Regulation and Governance in Europe. https://doi.org/10.1017/9781108609708.004

Ibrahimy, M. M., Norta, A., & Normak, P. (2023). Blockchain-based governance models supporting corruption-transparency: A systematic literature review. Blockchain: Research and Applications. https://doi.org/10.1016/j.bcra.2023.100186

Ibrahimy, M. M., Norta, A., & Normak, P. (2024). Blockchain-based governance models supporting corruption-transparency: A systematic literature review. Blockchain: Research and Applications, 5(2), 100186.

Integrating block chain technology to harness big data: Methods, obstacles, and future outlook. International journal of networks and systemsnull, . https://doi.org/10.30534/ijns/2023/011262023

ISO/IEC. (2020). ISO/IEC 22739:2020—Blockchain and distributed ledger technologies—Vocabulary.

Italy. (2005/2023). Decreto legislativo 7 marzo 2005, n. 82: Codice dell'Amministrazione Digitale (as amended), art. 17. Gazzetta Ufficiale della Repubblica Italiana.

Italy. (2019). Decree-Law No. 135 of 14 December 2018, converted by Law No. 12 of 11 February 2019, Article 8-ter.

Italy. (2019). Legge 11 febbraio 2019, n. 12 (di conversione del D.L. 135/2018), art. 8-ter: Tecnologie basate su registri distribuiti e smart contract. Gazzetta Ufficiale della Repubblica Italiana.

Italy. (2021). Decree-Law No. 82 of 14 June 2021 (establishing the National Cybersecurity Agency).

Italy. (2021). Piano Nazionale di Ripresa e Resilienza (PNRR). Rome: Presidenza del Consiglio dei Ministri.

Italy. (2022). Decreto-legge 30 aprile 2022, n. 36, convertito con modificazioni dalla Legge 29 giugno 2022, n. 79. Gazzetta Ufficiale della Repubblica Italiana.

Italy. (2023). Decreto legislativo 10 marzo 2023, n. 24: Attuazione della direttiva (UE) 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione. Gazzetta Ufficiale della Repubblica Italiana.

Italy. (2023). Decreto legislativo 31 marzo 2023, n. 36: Codice dei contratti pubblici (arts. 1, 15–16, 22–28, 62–63, 94–98, 108, 113–115, 220, 222). Gazzetta Ufficiale della Repubblica Italiana.

Italy. (2023). Decreto legislativo 31 marzo 2023, n. 36: Codice dei contratti pubblici. Gazzetta Ufficiale della Repubblica Italiana.

Italy. (2023). Legislative Decree No. 36 of 31 March 2023 (Codice dei contratti pubblici).

Italy. (2023). Legislative Decree No. 36 of 31 March 2023: Codice dei contratti pubblici. Gazzetta Ufficiale della Repubblica Italiana.

Janssen, M., Weerakkody, V., & Sivarajah, U. (2020). Digital transformation of government: A synthesis of research findings. Government Information Quarterly, 37(3), 101–113.

Janssen, M., Weerakkody, V., & Sivarajah, U. (2020). Theories used in blockchain research: A mapping review. Government Information Quarterly, 37(4), 101552. https://doi.org/10.1016/j.giq.2020.101552

Jones, A., & Pereira Neto, C. M. D. S. (2020). Combatting corruption and collusion in public procurement: Lessons from Operation Car Wash. SSRN. https://ssrn.com/abstract=3712858

Judge, W., McNatt, D., & Xu, W. (2011). The antecedents and effects of national corruption: A meta-analysis. Journal of World Business, 46(1), 93–103. https://doi.org/10.1016/j.jwb.2010.05.021

Jun, M.-S. (2018). Blockchain government - A next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity, 4, 1–12. https://doi.org/10.1186/s40852-018-0086-3

Jūrmalis, N., Berķe-Berga, A., & Urbāne, M. (2025). Advancing asset tokenization in the European Union and Latvia: A regulatory and policy perspective. Laws, 14(1), 7. https://doi.org/10.3390/laws14010007

Kálmán, J. (2024). Regulatory technology, platforms and data in public procurement: From digitization to algorithmic governance? Regional Law Review. (Advance online publication).

Kalman, M. (2024). Mosaics from the Legal Regulation of Blockchain Technology. Regional L. Rev., 215.

Kamalyan, V. (2020). Legal regulation of cryptocurrencies and blockchain technologies in Germany and Italy. Actual Problems of Russian Law, 116(7), 197–206. https://doi.org/10.17803/1994-1471.2020.116.7.197-206

Karisma, K., & Tehrani, P. M. (2022). Legal and Regulatory Landscape of Blockchain Technology in Various Countries. In Regulatory Aspects of Artificial Intelligence on Blockchain (pp. 52-81). IGI Global.

Kassen, M. (2022). Blockchain and e-government innovation: Automation of public information processes. Information Systems, 103, 101862. https://doi.org/10.1016/j.is.2021.101862

Kassen, M. (2023). Blockchain and digital governance: Decentralization of decision making policy. Review of Policy Research. https://doi.org/10.1111/ropr.12585

Katona, E., & Fazekas, M. (2024). Hidden barriers to open competition: Using text mining to uncover corrupt restrictions to competition in public procurement. (Working Paper series: GTI-WP/2024:01). ELTE & Government Transparency Institute.

Khamitov, Z., Knox, C., & Junusbekova, G. (2023). Corruption, public procurement and political instability in Kazakhstan. Central Asian Survey, 42(1), 89–108. https://doi.org/10.1080/02634937.2022.2072811

Khan, A. U. (2024). DISTRIBUTED LEDGER TECHNOLOGY: BEYOND CRYPTOCURRENCY–APPLICATIONS, CHALLENGES, AND FUTURE DIRECTIONS. Computer Science Bulletin, 7(02), 112-125.

Kingdomware Technologies, Inc. v. United States, 579 U.S. 162 (2016).

Kohler, J., & Dimancesco, D. (2020). The risk of corruption in public pharmaceutical procurement: How anti-corruption, transparency and accountability measures may reduce this risk. Global Health Action, 13(1), 1694745. https://doi.org/10.1080/16549716.2019.1694745

Kooiman, J. (2003). Governing as Governance. Sage.

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. Sensors, 22(14), 5274. https://doi.org/10.3390/s22145274

Kruessmann, T. (2021). The failure of transnational anti-corruption law. In Law, Development and Global Legal Pluralism (pp. 203–220). https://doi.org/10.4324/9781003174639-10

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038. https://doi.org/10.1016/J.TELPOL.2017.09.003

Kshetri, N. (2022). Blockchain's roles in fighting corruption and improving public sector efficiency in developing countries. IT Professional, 24, 4–8. https://doi.org/10.1109/mitp.2022.3224262

Kshetri, N. (2023). Blockchain's roles in strengthening public procurement systems. Government Information Quarterly, 40(1), 101692.

Kuipers, S. (2021). Rethinking anti-corruption efforts in international development. Journal of Financial Crime, 29(3), 934–948. https://doi.org/10.1108/JFC-08-2021-0176

Kuipers, S., & Verhey, V. (2023). How to deal with corruption if you want your economy to grow. Emerald Open Research, 5, 14. https://doi.org/10.35241/emeraldopenres.1114952.1

Latha, M., & Chinnaiyan, R. (2021, January). BlockchainAs a Service (BaaS) Framework for Government Funded Projects e-Tendering Process Administration and Quality Assurance using Smart Contracts. In 2021 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE.

Lessig, L. (1999). Code and other laws of cyberspace. Basic Books.

Lewis-Faupel, S., Neggers, Y., Olken, B. A., & Pande, R. (2016). Can electronic procurement improve infrastructure provision? Evidence from public works in India and Indonesia. American Economic Journal: Economic Policy, 8(3), 258–283.

Li, L., Liu, J., & Jia, P. (2021). SecTEP: Enabling secure tender evaluation with sealed prices and quality evaluation in procurement bidding systems over blockchain. Computers & Security, 103, 102188. doi:10.1016/j.cose.2021.102188

Li, X., Zhang, Y., & Chen, H. (2024). Blockchain-enabled supply verification for milestone-based payments in public contracts. Journal/Proceedings title. (Details to be completed).

Lin, M.-B., Pele, D., & Ren, R. (2024). Understanding blockchain technology. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4804484

Lingaraj, K., Harshitha, B., & Kavya, K. R. (2024, June). Smart Tender Contract Management System. In 2024 Second International Conference on Inventive Computing and Informatics (ICICI) (pp. 497-501). IEEE.

Lisciandra, M., Milani, R., & Millemaci, E. (2021). A corruption risk indicator for public procurement. European Journal of Political Economy, 69, 102141. https://doi.org/10.1016/j.ejpoleco.2021.102141

Little, T. D. (2013). Longitudinal structural equation modeling. Guilford Press.

Liu, C., & Mikesell, J. L. (2014). The impact of public officials' corruption on the size and allocation of U.S. state spending. Public Administration Review, 74(3), 346–359. https://doi.org/10.1111/puar.12212

Liu, M. (2021). Research on legal regulations of blockchain. Advances in Social Behavior Research. https://doi.org/10.54254/asbr.2021005

Löffler, E. (2003). Public management and governance. Routledge.

Lunardon, L., & Pagani, A. (2024, August). GOvNet: A Blockchain Overlay Network for Governments and Privacy-Oriented Applications. In 2024 IEEE International Conference on Blockchain (Blockchain) (pp. 105–112). IEEE.

Lyra, M., Curado, A., Damásio, B., Bação, F., & Pinheiro, F. (2021). Characterization of the firm–firm public procurement co-bidding network from the State of Ceará (Brazil) municipalities. Applied Network Science, 6(1), 1–10. https://doi.org/10.1007/s41109-021-00418-y

Lyra, M., Damásio, B., Pinheiro, F., & Bação, F. (2022). Fraud, corruption, and collusion in public procurement activities: A systematic literature review on data-driven methods. Applied Network Science, 7(1), 1–30. https://doi.org/10.1007/s41109-022-00523-6

Lyra, M., Damásio, B., Pinheiro, F., & Bação, F. (2022). Fraud, corruption, and collusion in public procurement activities: A systematic literature review on data-driven methods. Applied Network Science, 7, Article 45. https://doi.org/10.1007/s41109-022-00523-6

Mahmalat, M., & Maktabi, R. (2023). Digital governance in Lebanon: A political economy of stalled anti-corruption reforms. Middle East Law and Governance, 15(1), 28–59. https://doi.org/10.1163/18763375-15010002

Mahoney, J., & Thelen, K. (2010). Explaining Institutional Change: Ambiguity, Agency, and Power. Cambridge University Press.

Malik, S., Chadhar, M., Vatanasakdakul, S., & Chetty, M. (2021). Factors affecting the organizational adoption of blockchain technology: Extending the Technology–Organization–Environment (TOE) framework in the Australian context. Sustainability, 13(16), 9404. https://doi.org/10.3390/su13169404

Management Board of Cabinet. (2011). Broader Public Sector Procurement Directive.

Maolani, D. Y. (2024). Enhancing public service delivery through blockchain technology: A novel approach to transparent and efficient governance. https://doi.org/10.54783/jv.v16i1.1024

Marquette, H., & Peiffer, C. (2018). Grappling with the "real politics" of systemic corruption: Theoretical debates versus "real-world" functions. Governance, 31(3), 499–514. https://doi.org/10.1111/gove.12311

Martel Building Ltd. v. Canada, 2000 SCC 60.

Maume, P., & Kesper, F. (2023). The EU DLT pilot regime for digital assets. European Company Law. https://doi.org/10.54648/eucl2023039

Mazloum, H., Abdelkader, G., & Mazloum, N. (2022, November). Blockchain Overcomes Corruption: Towards Smart Institutions and Governance. In 2022 International Conference on Smart Systems and Power Management (IC2SPM) (pp. 80-84). IEEE.

Meijer, A. (2013). Understanding the complex dynamics of transparency. Public Administration Review, 73(3), 429–439.

Menezes, U. P. de, Oliveira, A. A. M. de, Filho, A. M., Costa, F. S., & Sebastiani, R. T. (2024). Direito Administrativo E Tecnologias Blockchain: Perspectivas Jurídicas Para A Administração Pública. IOSR Journal of Humanities and Social Science, 29(10).

Mergel, I. (2016). Agile innovation management in government: A research agenda. Government Information Quarterly, 33(3), 516–523.

Meza, O., & Pérez-Chiqués, E. (2020). Corruption consolidation in local governments: A grounded analytical framework. Public Administration, 98(4), 850–866. https://doi.org/10.1111/padm.12698

Mezquita, Y. (2021). RETRACTED CHAPTER: Public Tendering Processes Based on Blockchain Technologies. In International Symposium on Ambient Intelligence (pp. 247-250). Springer, Cham.

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. Business Horizons, 62(1), 35–45. https://doi.org/10.1016/J.BUSHOR.2018.08.012

Ministry of Economy and Finance. (2022). Linee guida tecnico-operative per il monitoraggio degli interventi PNRR e il sistema ReGiS. Rome: MEF.

Ministry of Infrastructure and Transport [MiSE]. (2019). Made in Italy – Traceability solution for supply chains. Retrieved from https://www.mimit.gov.it/images/stories/documenti/IBM-MISE-2019-INGLESE.pdf

Misran, A. (2024). Unraveling the impact of individual morality, arrogance, and greed on the risk of fraud in government procurement: Perspectives from local governments in South Kalimantan. Proceedings of the 2nd International Conference on Contemporary Risk Studies (ICONIC-RS 2023). https://doi.org/10.4108/eai.21-9-2023.2345660

Mo, P. H. (2001). Corruption and economic growth. Journal of Comparative Economics, 29(1), 66–79. https://doi.org/10.1006/jcec.2000.1703

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

Monteiro, F., & Correia, M. (2023, June). Decentralised autonomous organisations for public procurement. In Proceedings of the 1st International Workshop on Distributed Ledger Technology for Cyber-Physical Systems (DLCPS ’23) (pp. 1–6).

Muhammad, I., Wasiu, S., & Ahmad, M. (2023). Corruption and its impact on socio-economic development in selected countries of Africa. African Journal of Politics and Administrative Studies, 16(2). https://doi.org/10.4314/ajpas.v16i2.2

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. International Journal of Law and Management, 67(1), 37-55.

Mutungi, F. (2023). Digital anti-corruption typology for public sector. East African Journal of Information Technology, 6(1), 45–65.

Myint, U. (2000). Corruption: Causes, consequences and cures. Asia-Pacific Development Journal, 7(2), 33–58. https://consensus.app/papers/corruption-causes-consequences-and-cures-myint/01999e6e6e3c5d11909c2ac2d4619187/

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press.

National Archives and Records Administration, Records Management Regulations, 36 C.F.R. pts. 1220–1239.

National Institute of Standards and Technology (NIST). (2018/2022). Blockchain technology overview (NISTIR 8202 and subsequent technical updates).

National Institute of Standards and Technology. (2017). Digital identity guidelines (NIST SP 800-63-3).

National Institute of Standards and Technology. (2017). Digital Identity Guidelines (NIST SP 800-63-3). https://doi.org/10.6028/NIST.SP.800-63-3

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (Rev. 5, NIST SP 800-53). U.S. Department of Commerce.

National Institute of Standards and Technology. (2021). Protecting controlled unclassified information in nonfederal systems and organizations (Rev. 2, NIST SP 800-171). U.S. Department of Commerce.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.

Nese, A., & Troisi, R. (2019). Corruption among mayors: evidence from Italian court of cassation judgments. Trends in Organized Crime, 22(3), 298–323.

Ng, Y. K. I. (2025). The legal recognition and regulation of digital assets. Highlights in Business, Economics and Management. https://doi.org/10.54097/ybywwm42

Noble, E. (2020). Crypto-assets: Overcoming challenges to scaling – An EU approach. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3748343

Nodehi, A. R., Kalantari, R., & Moradi, S. (2022). Public sector blockchain adoption: Resistance, opportunity, and legitimacy. Information Polity, 27(1), 55–72. https://doi.org/10.3233/IP-210005

Ochigbo, A. D., Tuboalabo, A., Labake, T. T., Buinwi, U., Layode, O., & Buinwi, J. A. (2024). Legal frameworks for digital transactions: Analyzing the impact of Blockchain technology. Finance & Accounting Research Journal, 6(7), 1205-1223.

OECD. (2016). Preventing corruption in public procurement.

OECD. (2016). Preventing Corruption in Public Procurement. OECD Publishing.

OECD. (2020). Blockchain technologies and public procurement. OECD Working Papers on Public Governance. https://doi.org/10.1787/4cfe2f3e-en

OECD. (2020). Government at a Glance 2020. OECD Publishing.

OECD. (2022). Digital government review of Canada: Advancing digital government. OECD Publishing.

OECD. (2025). Implementing the OECD Recommendation on public procurement in OECD and partner countries. OECD Publishing.

Office of Federal Procurement Policy, 41 U.S.C. 1101–1131.

Office of Management and Budget & National Archives and Records Administration. (2022). Memorandum M-23-07: Update to transition to electronic records.

Office of Management and Budget (OMB). (2016/2021). Circular A-130: Managing Information as a Strategic Resource; Federal Data Strategy Action Plans.

Office of Science and Technology Policy (OSTP). (2022). Framework for the responsible development of digital assets.

Office of the Auditor General of Canada. (2021). Performance audit reports on federal procurement.

Office of the Privacy Commissioner of Canada. (2022). Privacy guidance for federal procurement and contracting.

Office of the Procurement Ombudsman. (2024). Annual report.

Owusu, E., Chan, A. P. C., & Hosseini, R. (2020). Impacts of anti-corruption barriers on the efficacy of anti-corruption measures in infrastructure projects: Implications for sustainable development. Journal of Cleaner Production, 246, 119078. https://doi.org/10.1016/j.jclepro.2019.119078

Padmanegara, O. H., Putri, R. K., Yuliani, R., & Masli, E. (2023). Blockchain and the public sector: Blockchain-based identity management systems for public services and the impact on privacy and security risks. 2023 International Conference on Digital Business and Technology Management (ICONDBTM), 1–6. https://doi.org/10.1109/ICONDBTM59210.2023.10326737

Palidauskaitė, J., & Ereminaitė, S. (2010). Corruption in public procurement: The definition and a case study (Part I). Public Policy and Administration, 32, 74–84.

https://consensus.app/papers/corruption-in-public-procurement-the-definition-and-a-case-palidauskait%C4%97-ereminait%C4%97/e001c2be477f580aa133a6eeb538f384

Patar, B. L. B., Akram, Hidayati, S. A., & Husnan, L. (2024). Determinants of goods/services procurement fraud with performance accountability as moderation in Central Lombok Regency Government. European Journal of Theoretical and Applied Sciences, 2(1), 108–120. https://doi.org/10.59324/ejtas.2024.2(1).12

Patil, D., & Bhosale, V. (2023). An overview of blockchain technology: Architecture, consensus, and future trends. International Journal of Advanced Research in Science, Communication and Technology, 22(1), 25–33. https://doi.org/10.48175/ijarsct-8158

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Persson, A., Rothstein, B., & Teorell, J. (2013). Why anticorruption reforms fail—Systemic corruption as a collective action problem. Governance, 26(3), 449–471. https://doi.org/10.1111/j.1468-0491.2012.01604.x

Piccardo, G. (2024). Blockchain technology and its potential to benefit public services provision: A short survey. Future Internet, 16(8), 290. https://doi.org/10.3390/fi16080290

Piccardo, G., Conti, L., & Martino, A. (2024). Blockchain technology and its potential to benefit public services provision: A short survey. Future Internet, 16(8), 290.

Pilkington, M. (2015). Blockchain technology: Principles and applications. In Research Handbook on Digital Transformations (pp. 225–253). https://doi.org/10.4337/9781784717766.00019

Pokharel, B. P., & Kshetri, N. (2024). blockLAW: Blockchain Technology for Legal Automation and Workflow--Cyber Ethics and Cybersecurity Platforms. arXiv preprint arXiv:2410.06143.

Popper, N. (2018, August 22). A Canadian government body has built an Ethereum blockchain explorer. CoinDesk. Retrieved from https://www.coindesk.com/markets/2018/08/22/a-canadian-government-body-has-built-an-ethereum-blockchain-explorer/

Post-employment restrictions for federal personnel, 18 U.S.C. 207.

Preukschat, A., & Reed, D. (Eds.). (2021). Self-Sovereign Identity: Decentralized digital identity and verifiable credentials. Manning.

Privacy Act of 1974, 5 U.S.C. § 552a.

Privacy Act, R.S.C., 1985, c. P-21.

Procurement Integrity Act, 41 U.S.C. 2101–2107.

Public Services and Procurement Canada. (2024). Supply Manual.

Public Services and Procurement Canada. (2024a). Supply Manual.

Public Services and Procurement Canada. (2024b). Ineligibility and Suspension Policy (Integrity Regime).

Public Services and Procurement Canada. (2024c). Contract Security Program and Security Requirements Check List.

Public Services and Procurement Canada. (n.d.). CanadaBuys (SAP Ariba).

Quah, J. (2021). Breaking the cycle of failure in combating corruption in Asian countries. Public Administration and Policy, 24(2), 153–167. https://doi.org/10.1108/PAP-05-2021-0034

Québec. (n.d.). Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR c A-2.1.

Québec. (n.d.). Act Respecting Contracting by Public Bodies, CQLR c C-65.1.

Radonjić, L., Bojić, L., & Novaković, M. (2024). Blockchain integration in public sector: A comprehensive review of economic and legal challenges. Ekonomika preduzeća, 72, 305-321.

Radonjić, L., Bojić, L., & Novaković, M. (2024). Blockchain integration in public sector: A comprehensive review of economic and legal challenges. Ekonomika Preduzeca. https://doi.org/10.5937/ekopre2406305r

Rahmani, M. K. I. (2022). Blockchain technology. In Blockchain Technology and Computational Excellence for Society 5.0 (pp. 1–19). IGI Global. https://doi.org/10.4018/978-1-7998-8382-1.ch002

Ramya, V., Mounisha, C., Mai, M. D., Kumari, M. N., & Saida, S. K. (2024). Blocktender: A trustworthy system. International journal of innovative science and research technologynull, . https://doi.org/10.38124/ijisrt/ijisrt24apr519

Rana, N., Dwivedi, Y., & Hughes, D. (2021). Analysis of challenges for blockchain adoption within the Indian public sector: An interpretive structural modelling approach. Information Technology & People, 35(2), 548–576. https://doi.org/10.1108/ITP-07-2020-0460

Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 15–17.

Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). (2016). Official Journal of the European Union.

Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. Official Journal of the European Union, L 57, 17–75.

Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility. Official Journal of the European Union, L 57, 17–75.

Regulation (EU) 2023/2854 of the European Parliament and of the Council (Data Act). (2023). Official Journal of the European Union.

Regulation (EU) 2024/1183 of the European Parliament and of the Council (European Digital Identity). (2024). Official Journal of the European Union.

Regulation (EU) No 910/2014 of the European Parliament and of the Council (eIDAS). (2014). Official Journal of the European Union.

Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF). Official Journal of the European Union, L 248, 1–22.

Rhodes, R. A. W. (2007). Understanding governance: Ten years on. Public Policy and Administration, 22(2), 1–19.

Roeck, D., Sternberg, H., & Hofmann, E. (2020). Distributed ledger technology in supply chains: A transaction cost theory perspective. International Journal of Production Research, 58(7), 2124–2141. https://doi.org/10.1080/00207543.2019.1657247

Rogleva, A. (2020). Preventing corruption in public procurements in domestic legal systems. Proceedings of the International Scientific Conference “Social Changes in the Global World”, 7(1), 71–79. https://doi.org/10.46763/scgw2071-20379r

Rose-Ackerman, S. (1975). The economics of corruption. Journal of Public Economics, 4(2), 187–203.

Rose-Ackerman, S. (1996). The political economy of corruption: Causes and consequences. World Bank Policy Research Working Paper Series, 1–4. https://doi.org/10.1596/11629

Rose-Ackerman, S. (2005). The challenge of poor governance and corruption. Revista Direito GV, 1(1), 207–266. https://doi.org/10.1017/CBO9780511581328.010

Rose-Ackerman, S., & Palifka, B. J. (2016). Corruption and government: Causes, consequences, and reform. Cambridge university press.

Rothstein, B. (2011). Anti-corruption: The indirect "big bang" approach. Review of International Political Economy, 18(2), 228–250.

Rothstein, B. (2021). Controlling corruption. Oxford University Press. https://doi.org/10.1093/oso/9780192894908.001.0001

Roy, S. (2023). The impact of blockchain technology on financial regulations and legal frameworks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4521762

Rules of the U.S. Government Accountability Office, Bid Protest Regulations, 4 C.F.R. pt. 21.

Rustiarini, N. W., Sutrisno, S., Nurkholis, N., & Andayani, W. (2019). Fraud triangle in public procurement: evidence from Indonesia. Journal of Financial Crime, 26(4), 951-968.

Rustiarini, N. W., T, S., Nurkholis, N., & Andayani, W. (2019). Why people commit public procurement fraud? The fraud diamond view. Journal of public procurement, 19(4), 345-362.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2018). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Sánchez-Graells, A. (2024). Digital technologies and public procurement: Gatekeeping and experimentation in digital public governance. Oxford University Press.

Sanka, A., Irfan, M., Huang, I., & Cheung, R. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. Computer Communications, 169, 179–201. https://doi.org/10.1016/j.comcom.2020.12.028

Sava, N.-A., & Dragoș, D. (2022). The legal regime of smart contracts in public procurement. Transylvanian Review of Administrative Sciences. (Article preprint available).

Sava, N.-A., & Dragoș, D. (2022). The Legal Regime of Smart Contracts in Public Procurement. Transylvanian Review of Administrative Sciences, (66E), 101–119. https://doi.org/10.24193/tras.66E.6

Sava, V., & Dragoș, D. C. (2022). Smart contracts in public procurement: Law and practice in the EU. In J. Carmona, G. Governatori, & A. Kő (Eds.), Business Process Management: Blockchain and Robotic Process Automation Forum (LNBIP, Vol. 433, pp. 105–122). Springer. doi:10.1007/978-3-031-06506-6_9

Savadatti, S. G., Krishnamoorthy, S., & Delhibabu, R. (2025). Survey of Distributed Ledger Technology (DLT) for Secure and Scalable Computing. IEEE Access, 13, 8393–8403.

Scholl, H., Pomeshchikov, R., & Bolívar, M. (2020). Early regulations of distributed ledger technology/blockchain providers: A comparative case study. In Proceedings of the 53rd Hawaii International Conference on System Sciences (pp. 218–227). https://doi.org/10.24251/hicss.2020.218

Secure Electronic Signature Regulations, SOR/2005-30 (Canada). (2005).

Securities Act of 1933, 15 U.S.C. §§ 77a–77aa.

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. Electronic Markets, 32, 1779–1794. https://doi.org/10.1007/s12525-022-00536-0

Selvanesan, H., & Rodrigo, N. (2024). Laws and policy initiatives in regulating blockchain and digital currencies. Journal of Science and Technology Policy Management, 15(1), 65–84. https://doi.org/10.1108/jstpm-12-2022-0199

Sharma, A., Gupta, R., Seth, J. K., & Garg, S. (2021). Blockchain and government. In Handbook of Green Computing and Blockchain Technologies. https://doi.org/10.1201/9781003107507-9

Sharma, S., Sengupta, A., & Panja, S. (2019). Mapping corruption risks in public procurement: Uncovering improvement opportunities and strengthening controls. Public Performance & Management Review, 42(4), 947–975. https://doi.org/10.1080/15309576.2018.1535984

Sharma, S., Sengupta, A., & Panja, S. (2019). Mapping corruption risks in public procurement: Uncovering improvement opportunities and strengthening controls. Public Performance & Management Review, 42(4), 947–975. https://doi.org/10.1080/15309576.2018.1535984

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts. Strategic Change, 26(5), 499–509. https://doi.org/10.1002/JSC.2150

Shu, J., Zou, X., Jia, X., Zhang, W., & Xie, R. (2021). Blockchain-based decentralized public auditing for cloud storage. IEEE Transactions on Cloud Computing, 10(5), 2366–2380. https://doi.org/10.1109/TCC.2021.3051622

Siddiqui, A., Balachandran, V., & Gupta, P. (2023). Blockchain-based framework for enhancing security and privacy in procurement [Working paper].

Siddiqui, A., Tansen, K., & Abdalla, H. (2023, October). Application of blockchain based e-procurement solution for mitigating corruption in smart cities using digital identities. In IFIP International Internet of Things Conference (pp. 87-100). Cham: Springer Nature Switzerland.

Siddiqui, S. T., Allfaqir, J., & Hong, J. (2023). Security risks in smart contract-based blockchain applications: Analysis and recommendations. In IFIPIoT 2023 — Internet of Things (LNCS 14277, pp. 59–74). Springer. https://doi.org/10.1007/978-3-031-40893-8_6

Signor, R., Love, P., & Ika, L. (2022). White collar crime: Unearthing collusion in the procurement of infrastructure projects. IEEE Transactions on Engineering Management, 69(6), 1932–1943. https://doi.org/10.1109/TEM.2020.2994636

Siino, M., Iezzi, S., & Gara, M. (2024). Corruption risk indicators in public procurement: A proposal using Italian open data. (Quaderni dell'antiriciclaggio 23). Banca d'Italia, Financial IntelligenceUnit.https://uif.bancaditalia.it/pubblicazioni/quaderni/2024/quaderno-23-2024/index.html

Small Business Act, 15 U.S.C. 631 et seq.; small business goals, 15 U.S.C. 644(g)(1).

Smart, A. (2018). The unbearable discretion of street-level bureaucrats. Current Anthropology, 59(S18), S117–S127. https://doi.org/10.1086/695694

Sobolewski & Allessie, 2021; Ba et al., 2023; Sava & Dragos, 2022; Wadegaonkar et al., 2024; Abdullah et al., 2022.

Sobolewski, M., & Allessie, D. (2021). Blockchain applications in the public sector: Investigating seven real-life blockchain deployments and their benefits. In Blockchain and the Public Sector: Theories, Reforms, and Case Studies (pp. 97-126). Cham: Springer International Publishing. Sousa, M. J. (2023). Blockchain as a driver for transformations in the public sector. Policy design and practicenull, . https://doi.org/10.1080/25741292.2023.2267864

Sørlie Lund, D. (2019). Special Issue on the Legal Remedies and Implications from the Fosen-Linjen Case· The Fosen-Linjen Saga-–A Norwegian Perspective. European Procurement & Public Private Partnership Law Review, 14(4).

Sotola, D. O., & Pillay, P. (2022). Thick concept but thin theories: A case for sector-based anti-corruption strategy. Oxford Development Studies, 50(4), 372–388. https://doi.org/10.1080/13600818.2022.2080812

Source: World Bank (2025). Worldwide Governance Indicators. https://info.worldbank.org/governance/wgi/

Sousa, M. J. (2023). Blockchain as a driver for transformations in the public sector. Policy Design and Practice. (Advance online publication). doi:10.1080/25741292.2023.2267864

Sousa, M. J. (2023). Blockchain as a driver for transformations in the public sector. Policy Design and Practice, 6(4), 415–432. https://doi.org/10.1080/25741292.2023.2267864

State smart-contract and blockchain statutes (e.g., Ariz. Rev. Stat. § 44-7061; Wyo. 2019 HB 70; Vt. 12 V.S.A. § 1913).

Sterman, J. D. (2000). Business dynamics: Systems thinking and modeling for a complex world. McGraw-Hill.

Suleiman, M. M. (2017). The politics of transparency and accountability in the age of open data. Public Performance & Management Review, 41(1), 1–31.

Sung, T. K., & Park, S. C. (2021). Digital trust and blockchain adoption in e-government: A cross-national comparison. Telecommunications Policy, 45(6), 102153. https://doi.org/10.1016/j.telpol.2021.102153

Szabo, J., Bernard, C., & Philip, L. (2024). Legal implications and challenges of blockchain technology and smart contracts. Computer, 12(2), 2024.

Tabish, S. Z. S., & Jha, K. N. (2011). Analyses and evaluation of irregularities in public procurement in India. Construction Management and Economics, 29(3), 261–274. https://doi.org/10.1080/01446193.2010.549138

Tan, E. (2023). The missing piece: The link between blockchain and public policy design. Policy Design and Practice, 6(4), 488–504. https://doi.org/10.1080/25741292.2023.2233160

Tan, E., Mahula, S., & Crompvoets, J. (2021). Blockchain governance in the public sector: A conceptual framework for public management. Government Information Quarterly. https://doi.org/10.1016/j.giq.2021.101625

Tanzi, V. (1998). Corruption around the world: Causes, consequences, scope, and cures. IMF Staff Papers, 45(4), 559–594. https://doi.org/10.2307/3867585

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 38, 105454. https://doi.org/10.1016/j.clsr.2020.105454

Tercon Contractors Ltd. v. British Columbia (Transportation and Highways), 2010 SCC 4.

Texas Government Code, ch. 2155 (state purchasing) and ch. 2260 (contract claims against the state).

Texas Public Information Act, Tex. Gov’t Code ch. 552.

Thomann, E., Ioannidis, G., Zgaga, T., & Schwarz, F. (2025). Explaining public sector corruption: The Hexagon Model. Governance. https://doi.org/10.1111/gove.70000

Torkanfar, E., Goodrum, P. M., & (co-authors). (2023). BidChain: A blockchain-based framework for fair and transparent public construction bidding. Journal of Construction Engineering and Management, 149(2), 04022173. doi:10.1061/JCEMD4.COENG-12970

Toufaily, E., Zalan, T., & Dhaou, S. ben. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. Information & Management, 58(6), 103444. https://doi.org/10.1016/j.im.2021.103444

Transparency International. (2024). Transparency, accountability, and integrity of public procurement systems. Anti-Corruption Helpdesk Answer. https://knowledgehub.transparency.org

Transparency International. (2025). What is corruption? Retrieved from https://www.transparency.org/en/what-is-corruption

Trautmann, L., & Lasch, R. (2021). Blockchain-based Smart Contracts in Procurement: A Technology Readiness Level Analysis. In Einkauf und Supply Chain Management (pp. 133-170). Wiesbaden: Springer Fachmedien Wiesbaden.

Treasury Board of Canada Secretariat. (2019, rev. 2023). Directive on Automated Decision-Making.

Treasury Board of Canada Secretariat. (2020). Directive on Automated Decision-Making.

Treasury Board of Canada Secretariat. (2020). Directive on Service and Digital.

Treasury Board of Canada Secretariat. (2021). Contracting Policy Notice: New Directive on the Management of Procurement. Government of Canada.

Treasury Board of Canada Secretariat. (2021). Directive on the Management of Procurement.

Treasury Board of Canada Secretariat. (2024). Directive on Automated Decision-Making (consolidated).

Trequattrini, R., Palmaccio, M., Turco, M., & Manzari, A. (2024). The contribution of blockchain technologies to anti-corruption practices: A systematic literature review. Business Strategy and the Environment. (Advance online publication).

Trequattrini, R., Palmaccio, M., Turco, M., & Manzari, A. (2024). The contribution of blockchain technologies to anti-corruption practices: A systematic literature review. Business Strategy and the Environment, 33(1), 4-18.

Troisi, R., & Alfano, G. (2023). Proximity and inter-firm corruption: A transaction cost approach. Small Business Economics, 60(3), 1105–1120. DOI: 10.1007/s11187-022-00649-y.

Troisi, R., Di Nauta, P., & Piciocchi, P. (2022). Private corruption: An integrated organizational model. European Management Review, 19(3), 476–486. https://doi.org/10.1111/emre.12489.

Tucker Act (bid protest jurisdiction), 28 U.S.C. 1491(b).

Tucker Act (bid protests), 28 U.S.C. 1491(b).

U.S. Food and Drug Administration. (2023). DSCSA Pilot Project Program. Retrieved from https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program

U.S. General Services Administration. (2023). Federal Acquisition Regulation (FAR) Subpart 4.5—Electronic commerce in contracting. https://www.acquisition.gov/far/subpart-4.5

U.S. General Services Administration. (2024). FAR Subpart 4.5—Electronic Commerce in Contracting. https://www.acquisition.gov/far/subpart-4.5

U.S. Government Accountability Office. (2011). Contract audits: Role in helping ensure effective oversight and reducing improper payments (GAO-11-331T).

UNCITRAL. (2012). UNCITRAL Legislative Guide on Public Procurement. United Nations.

Uniform Commercial Code, art. 2.

Uniform Electronic Commerce Act. (1999). Uniform Law Conference of Canada.

Uniform Electronic Transactions Act. (1999). Uniform Law Commission.

Uniform Guidance, 2 C.F.R. pt. 200; conflicts of interest, 2 C.F.R. 200.318; small/minority business utilization, 2 C.F.R. 200.321; domestic preferences, 2 C.F.R. 200.322; procurement methods, 2 C.F.R. 200.320; definitions and thresholds, 2 C.F.R. 200.1; subrecipient oversight, 2 C.F.R. 200.332; suspension and debarment, 2 C.F.R. 200.214.

Uniform Law Commission. (1999). Uniform Electronic Transactions Act (UETA). https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034

Uniform Law Commission. (1999). Uniform Electronic Transactions Act. https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034

Uniform Law Conference of Canada. (1999). Uniform Electronic Commerce Act.

Uniform Law Conference of Canada. (1999). Uniform Electronic Commerce Act.

United States Congress. (2000). Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001–7031.

United States Congress. (2000). Electronic Signatures in Global and National Commerce Act (ESIGN), 15 U.S.C. § 7001 et seq. https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter96

United States Congress. (2000). ESIGN, 15 U.S.C. §7001 et seq. https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter96

United States Courts. (2017/2019). Federal Rules of Evidence 901, 902(13), & 803(6). https://www.law.cornell.edu/rules/fre

United States Courts. (2019). Federal Rules of Evidence 901, 902(13), 803(6). https://www.law.cornell.edu/rules/fre

United States. (n.d.). Administrative Procedure Act, 5 U.S.C. § 553.

United States. (n.d.). Administrative Procedure Act, 5 U.S.C. §§ 551–559.

UNODC. (2013). Guidebook on anti-corruption in public procurement and the management of public finances.

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management, 54, 102120. https://doi.org/10.1016/j.ijinfomgt.2020.102120

Velasco, R., Carpanese, I., Interian, R., Neto, O. P., & Ribeiro, C. (2020). A decision support system for fraud detection in public procurement. International Transactions in Operational Research, 28(1), 27–47. https://doi.org/10.1111/itor.12811

Verma, S., & Sheel, A. (2022). Blockchain for government organizations: Past, present and future. Journal of Global Operations and Strategic Sourcing. https://doi.org/10.1108/jgoss-08-2021-0063

Virginia Public Procurement Act, Va. Code Ann. 2.2-4300 et seq.

Wadegaonkar, R. A., Srivastava, A., Mishra, B., Tatsavi, V., Mohite, S. G., & Jadhav, S. (2024, August). Smart Procurement and Contract Management Solution Using Blockchain. In 2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-6). IEEE.

Wamba, S. F., Wamba-Taguimdje, S. L., Lu, Q., & Queiroz, M. M. (2024). How emerging technologies can solve critical issues in organizational operations: An analysis of blockchain-driven projects in the public sector. Government Information Quarterly, 41(1), 101912.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266–2277. https://doi.org/10.1109/TSMC.2019.2895123

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 52, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Waxenecker, H., & Prell, C. (2024). Corruption dynamics in public procurement: A longitudinal network analysis of local construction contracts in Guatemala. Social Networks, 79, 154–167. https://doi.org/10.1016/j.socnet.2024.07.001

Weingärtner, T., Brucker, B., & Lopes, C. A. (2021). Prototyping a smart contract–based public procurement to fight corruption. Computers, 10(7), 85. doi:10.3390/computers10070085

Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke Law Journal, 67(2), 313–382.

Wibowo, W. S., & Yazid, S. (2023). Unveiling roadblocks and mapping solutions for blockchain adoption by governments: A systematic literature review. Interdisciplinary Journal of Information, Knowledge, and Management, 18, 547–581. (Open-access version).

Wibowo, W. S., & Yazid, S. (2023). Unveiling Roadblocks and Mapping Solutions for Blockchain Adoption by Governments: A Systematic Literature Review. Interdisciplinary Journal of Information, Knowledge, and Management, 18, 547-581.

Wittberg, E., & Fazekas, M. (2023). Firm performance, imperfect competition, and corruption risks in procurement: Evidence from Swedish municipalities. Public Choice, 197, 227–251. https://doi.org/10.1007/s11127-023-01102-8

World Trade Organization. (2014). Agreement on Government Procurement (revised GPA).

World Wide Web Consortium (W3C). (2023). Verifiable Credentials Data Model 2.0.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. SN Computer Science, 3(4), 268. https://doi.org/10.1007/s42979-022-01020-4

Xu, X., Qian, Y., Lu, Y., Zhang, H., & Wu, J. (2021). A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective. Advances in Civil Engineering, 2021, 6623954. https://doi.org/10.1155/2021/6623954

Yadav, A., Singh, N., & Kushwaha, D. (2023). Evolution of blockchain and consensus mechanisms & its real-world applications. Multimedia Tools and Applications, 1–46. https://doi.org/10.1007/s11042-023-14624-6

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. National Institute of Standards and Technology, NIST IR 8202. https://doi.org/10.6028/NIST.IR.8202

Yeoh, P. (2017). Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance, 25(2), 196–208. https://doi.org/10.1108/JFRC-08-2016-0068

Yu, J. (2024). Exploration of the application of blockchain in e-government: Opportunities and risks coexist. Information Services and Use, 44(3), 255–266.

Yusof, H. M., Yusof, D. M., & Adnan, N. M. (2024). The role of the principal-agent-client model in understanding corruption in the public procurement sector in Malaysia. Intellectual Discourse, 32(1), 145–160. https://doi.org/10.31436/id.v32i1.2026

Zachry Constr. Corp. v. Port of Houston Auth., 449 S.W.3d 98 (Tex. 2014).

Zafar, A. (2025). Reconciling blockchain technology and data protection laws: Regulatory challenges, technical solutions, and practical pathways. Journal of Cybersecurity, 11, tyaf002. https://doi.org/10.1093/cybsec/tyaf002

Zamani, E., He, Y., & Phillips, M. L. F. (2018). On the security risks of the blockchain. Journal of Computer Information Systems, 60(6), 495–506. https://doi.org/10.1080/08874417.2018.1538709

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. Fordham Journal of Corporate & Financial Law, 23(1), 31–103.

Zhang, Y., Gong, B., & Zhou, P. (2024). Centralized use of decentralized technology: Tokenization of currencies and assets. Structural Change and Economic Dynamics, 71, 249–260. https://doi.org/10.1016/j.strueco.2024.06.006

Zhang, Y., Li, X., & Zhang, Q. (2022). Adaptive policy transfer in digital government: Organizational readiness and capacity for innovation. Government Information Quarterly, 39(3), 101732.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557–564). https://doi.org/10.1109/BIGDATACONGRESS.2017.85

Zhuk, A. (2025). Beyond the blockchain hype: Addressing legal and regulatory challenges. SN Social Sciences, 5(2), 44. https://doi.org/10.1007/s43545-024-01044-y

Zweig, A., & Carroll, J. (2022). Smart contracts and Canadian law: Legal considerations in digital procurement. Canadian Journal of Law and Technology, 20(1), 55–74.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE security and privacy workshops (pp. 180–184). IEEE.