

UNIVERSITÀ DEGLI STUDI DI SALERNO
Dipartimento di Scienze Economiche e Statistiche



CORSO DI DOTTORATO DI RICERCA
in
Economia e politiche dei mercati e delle imprese
Curriculum: *Economia del Settore Pubblico*

XXXVIII ciclo

**A New Institutional Paradigm:
A Multi-Level Analysis of Blockchain, Incentives, and Coordination in the Public Sector**

PHD THESIS

Coordinatore

Ch.ma Prof.ssa Alessandra AMENDOLA

Tutors

Ch.ma Prof.ssa Bruna BRUNO (UNISA)

Ch.mo Prof. Vincenzo VESPRI (UNIFI)

Dottorando (n. matr 8861200007)

Dott. Angelo MURANO

A mia madre, custode dei miei sogni.
A mio padre, custode della mia concretezza.
A mio fratello, legame tra queste due anime.

ABSTRACT

This dissertation investigates whether blockchain can be meaningfully conceptualized as an institutional technology and how such a perspective may help explain its evolving role in the public sector. While blockchain is often promoted for its potential to enhance transparency, efficiency, and trust in government services, large-scale adoption in the public sector remains limited, suggesting that technological innovation alone may not be sufficient to drive transformation. Drawing on insights from innovation studies, institutional economics, organizational theory, and computer science, the research adopts a multi-level analytical framework to examine how blockchain's technological features intersect with governance structures, organizational arrangements, and incentive mechanisms.

Across five interconnected studies, the work highlights that blockchain's trajectory in the public sector appears strongly shaped by institutional conditions. A systematic review identifies barriers rooted not only in technical challenges but also in regulatory uncertainty, organizational resistance, and capability gaps. A cross-country empirical analysis suggests that blockchain diffusion correlates more closely with indicators of governance quality and institutional readiness than with conventional drivers of technology adoption, pointing to a diffusion pattern distinct from that of more established general-purpose technologies. A theoretical analysis of the organizational model enabled by blockchain technology - here labelled as the V-Form - provides a conceptual lens for understanding how decentralized coordination structures may emerge. Complementary analyses of consensus mechanisms and validator incentives further suggest that blockchain's technical architecture can perform governance functions by embedding rules and incentive structures directly into software protocols.

Taken together, the findings suggest that blockchain may be viewed not only as a digital tool but also as a potential institutional innovation whose prospects depend on the alignment between technical design and institutional context. This perspective offers both conceptual contributions and practical implications for policymakers seeking to navigate the future of blockchain in public-sector governance.

KEYWORDS:

Blockchain; Institutional Technology; Public Sector; Blockchain Governance; Organizational Innovation; Incentive Compatibility; Decentralization; Distributed Ledger Technology (DLT); Evolutionary Economics; Economic of Innovation; Technological Paradigms; Technological Trajectories; Agency Theory; Blockchain Economics; Digital Transformation; Game Theory; General Purpose Technology (GPT); Multilevel Framework; Smart Contracts; Consensus Mechanisms; V-Form Organization; Governance Design; Micro-Meso-Macro Analysis; Coordination Costs; Institutional Change; Validator Incentives; Permissioned vs. Permissionless Networks; Comparative Innovation; Quantitative Research; Text Mining; Trust-by-Design; Public-Private Consortia; Digital Institutional Infrastructure; Innovation Diffusion; Policy Readiness; Institutional Barriers; Governance Mechanisms; Regulatory Uncertainty.

ACKNOWLEDGEMENTS

I would like to express my gratitude to Professor Alessandra Amendola, Coordinator of the PhD programme, and to the academic and administrative community of the Department of Economics and Statistics at the University of Salerno, whose human qualities complement and often exceed their already remarkable professional expertise.

Above all, my deepest thanks go to those who have been a constant source of guidance and support throughout this journey.

To Bruna Bruno and Vincenzo Vespri, whom I have always listened to with gratitude: they were not just supervisors, but a steady and caring presence.

There are people who pass on knowledge, and people who show, through the way they live and act, that knowledge can truly transform those who receive it. Their words carry the weight of a road they have walked, of joys and struggles they have known, and for that reason they are never abstract.

I thank them for opening horizons I could not have seen on my own, for pointing out new possibilities while always entrusting me with the freedom, priceless freedom, to choose my own direction. Their example shaped this journey more than any notion or lesson, turning an academic task into a path of personal growth.

And if this journey leaves me with one hope, it is this: that one day, in my own small way, I may be for someone what they have been, what they are and what they will be for me.

AUTHOR'S FOREWORD

This dissertation combines published and original research to present a coherent and progressive investigation into blockchain as an institutional technology in the context of public sector innovation. Chapters 1 and 5 are based on peer-reviewed international journal articles co-authored with my doctoral supervisors, Professor Bruna Bruno and Professor Vincenzo Vespri. In these joint works, my principal contribution was the conception and development of the core analytical and theoretical frameworks. The supervisors' role consisted of providing scientific guidance and supporting the refinement of methodologies and analysis.

Complementing these published studies, Chapters 2, 3, and 4 introduce entirely new and unpublished research that extends the scope of the investigation and offers substantial original insights. Together, the five chapters form an integrated structure that maintains continuity in the research narrative while demonstrating my independent contribution to advancing knowledge in the field. This approach allows the thesis to benefit from the rigor of peer-reviewed scholarship while simultaneously presenting original research outcomes.

Table of contents

ABSTRACT	3
ACKNOWLEDGEMENTS	5
AUTHOR’S FOREWORD	5
<i>Introduction</i>	8
CHAPTER 1	14
<i>Barriers to blockchain adoption in public organizations</i>	14
CHAPTER 2	19
<i>Blockchain as an Institutional Technology? A Comparative Analysis of Digital Innovation in the European Public Sector</i>	19
2.1 Introduction	19
2.2 Theoretical framework.....	23
2.2.1 Technological paradigms and trajectories	23
2.2.2 Blockchain as an institutional technology	24
2.2.3 Blockchain vs AI: different paradigms and adoption logics	26
2.3 Data and Methodology.....	28
2.3.1 Data source and scope	28
2.3.2 Exploratory analysis: clustering countries by adoption patterns	29
2.3.3 Econometric strategy	30
2.4 Results.....	33
2.4.1 Country clusters: Active vs. Less-Active innovators	33
2.4.2 Baseline regression results	36
2.4.3 Extended Regression Results: Interaction Effects and Cluster Factor	38
2.4.4 Summary of Empirical Findings	43
2.5 Discussion	45
2.6 Policy implications	46
2.7 Conclusion.....	46
CHAPTER 3	49
<i>The evolution of organizations and blockchain: a multilevel framework</i>	49
3.1 Introduction	49
3.2 Evolution of organizational forms	50
3.2.1 U-Form	50
3.2.2 M-Form.....	51
3.2.3 Virtual Organization.....	51
3.2.4 V-Form.....	52
3.3 Methodology: Micro–Meso analytical framework	53
3.3.1 Meso-organizational model: cost structures of different forms	55
3.3.2 Organizational cost components	56
3.3.3 Formal representation of organizational archetypes	56
3.3.4 Interpretation and results	60
3.3.5 Micro-individual model: from validator behaviour to emergent organizational trust	61
3.3.6 Endogenizing trust: micro-level dynamics in validator behaviour	62
3.3.7 Aggregation mechanism: from behaviour to trust	63
3.3.8 Linking micro behaviour to meso outcomes.....	63

3.4 Discussion: blockchain as institutional technology	64
3.5 Conclusions	66
3.6 Future insights	67
CHAPTER 4	69
<i>Blockchain as economic infrastructure: incentives and governance mechanisms</i>	<i>69</i>
4.1 Introduction	69
4.2 Principal-Agent Dynamics in Blockchain Platforms	73
4.2.1 Blockchain governance structures and performances	75
4.2.3 BC structure and the concept of trust	77
4.2.4 BC performance output	78
4.3 The agency problem and the consensus protocols	79
4.3.1 The consensus protocols	80
4.3.2 Costs and rewards	84
4.3.3 BC design and the agency problem	84
4.4 Asymmetric information and governance mechanism in permissioned BCs	85
4.5 Conclusions	87
CHAPTER 5	89
<i>Incentives for Sustainable Blockchain Governance – A Game-Theoretic Analysis</i>	<i>89</i>
5.1 Institutional and policy implications of incentive compatibility in public-sector blockchains	93
5.1.1 Validator incentives, governance design, and public procurement	95
5.2 Micro-foundations and the conditional institutional claim	95
<i>Concluding remarks</i>	<i>98</i>
<i>References</i>	<i>101</i>
ARTICLES	108

Introduction

Blockchain technology has gained significant attention for its potential to transform public sector services by enhancing transparency, efficiency, and trust. Governments and public organizations worldwide have begun experimenting with blockchain-based solutions in areas such as land registries, digital identity management, healthcare records, public finance, and electronic voting. These pilot initiatives aim to improve the integrity and traceability of administrative processes.

However, despite this technological promise, large-scale adoption in the public sector remains limited. Most implementations are still confined to isolated trials and face substantial barriers. Technical issues - such as interoperability with legacy systems and the shortage of specialized skills - combine with organizational and institutional challenges, including regulatory uncertainty and cultural resistance to change within public administrations. These obstacles highlight a critical point: the mere availability of a novel technology does not ensure its uptake in government contexts. Realizing blockchain's transformative potential requires addressing deeper issues of coordination, capability, trust and clarifying who designs, controls, and maintains the governance arrangements that digital technologies instantiate within public organizations and across public-private ecosystems.

Public-sector blockchain initiatives should therefore be interpreted against the longer historical pattern of digital transformation in government. Over the past three decades, public administrations have repeatedly pursued modernization through technology in successive waves, from early computerization and database-driven reforms, to the rise of e-government in the 1990s–2000s, to the more recent agenda of digital government. Each wave has been accompanied by promises of efficiency, transparency, and citizen-centric redesign, yet empirical and policy debates have also emphasized persistent implementation gaps, uneven outcomes, and recurring governance dilemmas. A central lesson emerging from this literature is that public-sector digitalization is rarely a purely technical substitution: it is an institutional process shaped by legal constraints, legacy infrastructures, organizational cultures, and political accountability, often producing path-dependent trajectories rather than immediate discontinuities ([Dunleavy, 2006](#); [Fountain, 2001](#)).

Within this pattern, an especially salient tension concerns the boundary between technological modernization and the preservation (or erosion) of endogenous state capability. In many contexts, core digital transformation tasks - system design, procurement, implementation, and evaluation - have been heavily intermediated by external actors, including large IT vendors and consulting firms. This can accelerate delivery in the short run, but may also generate long-run dependencies, information asymmetries, and a weakening of in-house expertise and “institutional memory”. In their recent account of the consulting industry's role in government, ([Mazzucato & Collington, 2026](#)) argue that persistent reliance on external

consultancies can infantilize public institutions by displacing internal learning and by blurring lines of responsibility, thereby increasing conflicts of interest and reducing strategic agency.

A second, closely related development concerns the political economy of data and digital infrastructures. Contemporary digital public services increasingly depend on large-scale data infrastructures, cloud platforms, and algorithmic tools. At the same time, the consolidation of data and computational capabilities among a limited number of global firms has raised concerns about market power, transparency, and democratic accountability. Calzada's notion of "data-opolies" frames this concentration as a structural challenge for "datafied democracies", where the control of data infrastructures can condition competition, policy autonomy, and even the informational foundations of democratic governance (Calzada, 2024).

Blockchain emerges at the intersection of these two dynamics: (i) the long-run struggle to modernize government without hollowing out public capability, and (ii) the growing concern that digital infrastructures and data governance are becoming structurally centralized. In the most optimistic interpretation, blockchain-based systems could support new forms of transparency and accountability by embedding auditability, traceability, and rule enforcement into shared digital infrastructures. More ambitiously, if governance rules and incentive mechanisms can be credibly encoded and collectively validated, blockchain could contribute to institutional arrangements in which individual incentives are aligned with collective objectives, potentially reducing conflicts of interest and limiting the discretionary power of intermediaries. Yet an equally plausible risk is that blockchain adoption reproduces familiar patterns of externalization, where this technology is procured as an off-the-shelf solution, implemented and governed primarily by external vendors or consortia, with limited endogenous learning inside public administrations. The core analytical challenge is therefore not whether blockchain is innovative in a technical sense, but whether - and under what governance conditions - it can foster durable institutional reconfiguration rather than another cycle of outsourced modernization.

These practical uncertainties are mirrored in the academic debate, and, more broadly, in competing interpretations of what "digital transformation" means when the object being transformed is the institutional machinery of the state. Early literature often positioned blockchain as a General Purpose Technology (GPT) (Kane, 2017), comparable to artificial intelligence or the internet, an innovation expected to generate efficiency gains across multiple domains. This perspective was reinforced by blockchain's foundational role in cryptocurrency systems, which underscored its broad, general-purpose characteristics.

More recent studies, however, proposes an alternative view: blockchain can be understood as an institutional technology (Davidson, De Filippi, & Potts, 2018). From this standpoint, blockchain is not simply a neutral IT tool for data management. Instead, it embeds governance functions and trust mechanisms directly within its technical architecture. By automating rule enforcement and aligning participant behaviour through code (Berg et al., 2017), blockchain

introduces a new approach to institutional design, one that can “industrialize trust”. Rather than merely digitizing existing processes, blockchain has the capacity to redefine the underlying rules by encoding agreements, roles, and incentives into a decentralized, immutable ledger. In this sense, blockchain offers a way to engineer institutions, the formal and informal rules governing organizational and economic interactions, within a distributed network. This perspective leads to the central research question of this dissertation: to what extent - and under what institutional conditions, governance arrangements, and capability constraints - can blockchain be conceptualized as an institutional technology, particularly in the context of public sector transformation?

This dissertation treats blockchain as “institutional technology” as a conditional hypothesis: blockchain can function as an institutional innovation only when it is embedded within governance designs and organizational arrangements that public institutions can understand, steer, and progressively internalize through endogenous capability building. In other words, the institutional character of blockchain is not ontological, but relational and implementation-dependent.

In this perspective, several of the barriers discussed in the public-sector literature can be interpreted not merely as obstacles to implementation, but as indicators of limited public capability to design and sustain incentive-compatible institutional infrastructures. This dissertation therefore treats blockchain adoption primarily as a problem of institutional coordination and governance design, rather than as a purely technological transition.

Addressing this question requires a multidisciplinary and multi-level analytical approach. The research draws on innovation studies, institutional economics, organizational theory, and computer science to examine how blockchain’s technological evolution intersects with processes of governance and institutional change. Specifically, the dissertation adopts a multi-level perspective inspired by socio-technical and innovation frameworks (Dopfer, 2005), which emphasize that transformative change results from interactions across different analytical levels, and that such interactions are best understood when situated within the longer-run institutional trajectory of public-sector digitalization outlined above.

In this dissertation, the analysis unfolds across three interconnected levels. At the macro level, examined in Chapter 2, the study explores the broader socio-economic and policy environment that shapes the diffusion of blockchain in the public sector. The macro-level perspective is supported by an econometric analysis, which provides a data-driven foundation for the theoretical framework developed in the subsequent chapters.

The meso level, addressed in Chapter 3, focuses on organizational and institutional dynamics. This level considers the emergence of new organizational forms, as well as evolving governance arrangements within and between public institutions. It highlights how institutional structures mediate the translation of macro-level forces into concrete strategies and coordination mechanisms.

Finally, the micro level, discussed in Chapter 3 and in particular Chapter 5, examines the behaviour of individual actors and technological components. This includes incentive dynamics among blockchain network participants and the decision-making processes of organizations piloting specific blockchain applications.

Taken together, these three levels provide an integrated perspective that captures both the granular, agent-level mechanisms and the wider structural forces influencing the trajectory of blockchain adoption and implementation in governmental contexts.

This multi-level lens is essential for understanding blockchain's dual nature as both a technical artifact and an institutional phenomenon. It enables the research to link questions of technological design - for example, how consensus mechanisms address coordination problems - with questions of institutional context, such as how laws, norms, and organizational capacities influence blockchain adoption in the public sector.

The scope of this dissertation is intentionally broad, reflecting the interdisciplinary nature of the research problem. Rather than focusing on a single case or specific use-scenario, the work brings together multiple studies to examine whether - and how - blockchain operates as an institutional innovation in the public sector. The investigation begins by mapping the existing state of knowledge and then progressively moves from macro- and meso-level patterns toward micro-level mechanisms.

Chapter 1 develops a reasoned and integrative reflection on the findings of the corresponding published study, which is reproduced in full in the Articles section, and uses them to establish the conceptual foundation of the dissertation. The chapter reinterprets the literature on blockchain applications in the public sector in light of the broader research trajectory pursued in this thesis. It systematically reviews the main technical, organizational, and regulatory barriers to adoption, showing how issues such as interoperability, governance, and cultural resistance take on distinctive forms within governmental contexts. In doing so, it highlights a critical gap in existing research: the need for an economic and organizational perspective capable of capturing the specific institutional dynamics of the public sector. The chapter therefore frames “barriers” not simply as implementation obstacles, but as observable expressions of deeper capability and governance constraints that shape the conditions under which blockchain may evolve into a genuine institutional innovation rather than remain an externally supplied technological add-on.

Building upon these insights, Chapter 2 conducts a comparative, data-driven investigation to test the hypothesis of blockchain as an “institutional technology” (Davidson et al., 2018) at a large scale. This study quantitatively analyses blockchain adoption across a sample of countries and compares these patterns with the diffusion of a more conventional general-purpose technology – Artificial Intelligence (AI) - in similar public sector contexts. By using AI as a benchmark, Chapter 2 evaluates whether blockchain follows a distinct adoption logic shaped by institutional and governance variables, rather than the diffusion patterns typical of standard technologies. The econometric analysis investigates how factors such as

technological capacity, R&D investment, public-sector size, and governance quality correlate with blockchain-based innovation, and how these correlations differ from those associated with AI. The findings provide empirical exploratory evidence on whether blockchain diverges from typical innovation trajectories, thereby contributing to the understanding of its institutional character without presuming that observed differences necessarily imply a full paradigmatic discontinuity.

Shifting to the meso-level, Chapter 3 introduces an original theoretical model of organizational innovation enabled by blockchain. It develops the concept of the “V-Form” organization (Berg et al., 2020), a new organizational paradigm grounded in decentralized trust and algorithmic governance. The chapter traces the evolution of organizational forms - from traditional hierarchical models like the U-form and M-form - to a blockchain-enabled structure characterized by distributed coordination. The V-Form model explains how independent actors, across or within organizations, can collaborate and establish trust through transparent protocols and shared ledgers rather than through hierarchical authority or contractual enforcement. By integrating micro-level incentive analysis with meso-level organizational design, Chapter 3 offers a multi-level framework for understanding how blockchain reshapes coordination costs and redistributes trust, opening possibilities for new public-private collaborations and decentralized administrative networks. This theoretical contribution advances the literature on organizational innovation while offering practical insight into what decentralized public organizations could look like in practice.

The dissertation then turns to the technical-economic mechanisms that allow blockchain to function as a governance system. Chapter 4 reframes blockchain’s technical architecture - particularly its consensus mechanisms - in terms of economic and institutional governance. By linking concepts from computer science to institutional economics and agency theory, the chapter argues that consensus algorithms (e.g., Proof of Work, Proof of Stake, and voting-based protocols) operate as institutional rules encoded in software. These rules coordinate distributed actors, align incentives, and mitigate risks of opportunistic or malicious behaviour in the absence of centralized authority. The chapter compares different blockchain architectures, contrasting open, permissionless systems with permissioned or consortium models, and shows how each approach embeds distinct modes of trust, enforcement, and incentive alignment. This analysis demonstrates that seemingly technical design choices carry institutional implications, and positions blockchain consensus protocols as a new economic infrastructure for coordination, blurring the boundary between technology and governance.

Finally, Chapter 5 provides a reasoned and integrative discussion of the main results of the related published article, which is included in full in the Articles section at the end of the thesis. The chapter revisits the formal analysis of validator incentives from a broader perspective, situating the game-theoretic model within the dissertation’s overarching investigation of governance design and institutional capacity. By examining how alternative incentive schemes — such as proof-based mechanisms or reputation- and vote-based structures — affect

network sustainability and security, the analysis shows how incentive architecture shapes the equilibrium behaviour of self-interested participants. This reflection underscores the principle of incentive compatibility while linking micro-level coordination mechanisms to macro-level institutional outcomes. In this way, the chapter contributes not only practical insights for the design of blockchain governance systems that reduce free-riding and security vulnerabilities, but also reinforces the dissertation's central argument: institutional performance depends on the configuration of incentives and governance arrangements rather than on technological adoption per se.

Taken together, these five studies form a cohesive examination of blockchain as an institutional technology. Each chapter addresses the central research question from a different angle, ranging from existing challenges, to diffusion patterns, to new organizational forms, to the governance logic embedded in consensus and incentives. The concluding section integrates these findings, reflecting on their implications for public sector innovation and technological paradigms. It highlights the dissertation's theoretical contributions, such as advancing innovation diffusion models and institutional theory and its practical relevance for policymakers and public managers. The conclusion also acknowledges the study's limitations and outlines directions for future research, recognizing that blockchain's institutional impact is still evolving and that its ability to support genuine public-sector transformation ultimately depends on whether public institutions can build and retain the capabilities required to steer, govern, and learn from blockchain-based systems over time.

CHAPTER 1

Barriers to blockchain adoption in public organizations

This section provides a comprehensive state-of-the-art review of barriers to blockchain adoption in public organizations, examined through an economic and organizational lens. It constitutes a commented and analytically structured synthesis of the original article reproduced in the Appendix,¹ and is specifically designed to clarify the scope and research objectives that guide the subsequent chapters. By revisiting the literature in this integrative manner, the chapter delineates the main analytical directions that underpin the dissertation's broader investigation of blockchain as a potential institutional technology. It shows that diffusion in government is not merely a technical issue but a multifaceted challenge involving interoperability, skills, organizational culture, institutional trust, and governance structures. By systematically identifying these obstacles and emphasizing differences from private-sector contexts, the review establishes a critical foundation for the broader thesis. The insights highlight why public-sector blockchain initiatives require carefully designed incentives, capacity-building, and governance frameworks, themes explored later in greater empirical and theoretical depth. The chapter is not only a catalogue of obstacles but also a diagnostic map of the institutional and capability constraints that condition whether blockchain can become a genuine institutional innovation in the public sector.

Blockchain technology is widely promoted for its potential to enhance transparency, efficiency, and trust in public administration. Governments worldwide have launched pilot projects in land registries, digital identity, healthcare, public finance, and e-voting to improve data integrity and process traceability. Yet real-world adoption remains limited: implementations are few, isolated, and often experimental. Availability of the technology alone does not guarantee uptake; deeper issues of coordination, capability, and trust must be addressed. Promised benefits such as improved security, accountability, and efficiency are counterbalanced by persistent organizational and institutional hurdles. Interoperability gaps with legacy systems, shortages of specialized skills, unclear regulations, and cultural resistance to change continue to impede deployment in public governance contexts. Blockchain's potential to "industrialise trust" by embedding rules and incentives in code (Berg et al., 2017) will remain unrealized in government settings unless these barriers are rigorously understood and overcome.

Public-sector digitalization is historically characterized by recurring promises of transparency and efficiency, but also by persistent governance dilemmas concerning sourcing, coordination,

¹ Murano, A., Bruno, B., & Vespri, V. (2025). Blockchain barriers in public organizations: A systematic literature review. *Socio-Economic Planning Sciences*, 102364.

and the preservation of endogenous administrative capabilities. In this context, the adoption of blockchain should not be interpreted as a purely technical choice. Rather, it is embedded in - and constrained by - the institutional conditions under which public organizations procure, govern, and learn from complex digital infrastructures.

The purpose of this chapter is therefore twofold. First, it synthesizes the literature on blockchain initiatives and barriers in public organizations using a systematic approach. Second, it leverages that synthesis diagnostically: the recurrent barriers mapped in the literature can be read as observable manifestations of deeper constraints on public-sector capability. Put differently, “barriers” are not merely implementation frictions, but they often reveal where institutional arrangements, governance routines, and organizational competences are misaligned with what blockchain-based systems require.

This diagnostic reading matters for the dissertation’s core claim. If blockchain is to be conceptualized as an institutional technology in the public sector, this characterization cannot be treated as intrinsic or automatic. It must be understood as conditional on the ability of public institutions to (i) specify institutional objectives and governance rules, (ii) choose and steer technical designs consistent with those objectives, and (iii) progressively internalize knowledge rather than relying on purely transactional acquisition from external providers. The remainder of the chapter maps the barrier landscape precisely to clarify what these conditions entail in practice.

Despite growing interest, prior studies have underexamined the public-sector perspective. Early academic discourse often framed blockchain as a general-purpose technology, focusing on technical performance and assuming broad applicability similar to other IT innovations. More recently, scholars have argued that blockchain functions as an “institutional technology,” directly embedding governance functions and trust mechanisms into its architecture (Davidson et al., 2018). This view suggests that economic and organizational factors—rules, incentives, institutional context—are as critical as technical properties in shaping outcomes. However, existing literature reviews rarely adopted such an economic–organizational lens or distinguished the specific conditions of the public sector, often failing to differentiate government use-cases from private-sector ones. Earlier reviews and case studies highlighted potential benefits and generic challenges, but concrete empirical analyses of public-sector implementation barriers remained scarce (Batubara et al., 2018; Riyoldi et al., 2023; Tan et al., 2022). A knowledge gap therefore persisted regarding how and why public organizations struggle with blockchain adoption beyond purely technical issues.

To ensure methodological rigor, a Systematic Literature Review (SLR) was conducted in accordance with established PRISMA guidelines (Cinar, 2019). A full and detailed description of the research design and methodological procedures is provided in the original published article reproduced in the Appendix (see Section 3), while the present chapter offers a condensed account tailored to the dissertation’s analytical objectives. The search focused on peer-reviewed studies published within roughly the last five years, reflecting the rapid evolution of blockchain research. Using keywords related to “public sector,” “blockchain,” “challenges,”

“barriers,” “organizational,” and “technical,” major scholarly databases - including Scopus, Web of Science, and IEEE Xplore - were queried. After screening titles, abstracts, and full texts, 37 articles were identified that directly examined blockchain use in public-sector contexts and the obstacles to its implementation. To ensure quality and comparability, only English-language academic publications were included. Insights were extracted through qualitative thematic analysis, coding use cases, cited challenges, and proposed solutions. To complement this interpretive approach with greater objectivity, a Python-based text-mining procedure was also applied. Term-frequency analysis and topic modelling were used to identify recurrent themes such as “interoperability”, “scalability”, “trust”, “privacy”, “governance” and “regulation”. These results helped validate that the classification of barriers reflected consistent patterns in the literature rather than solely subjective assessment. The findings were ultimately organized into broad categories, distinguishing between technical-operational barriers and organizational-institutional barriers, with additional overlapping subcategories such as regulatory/legal constraints and cultural or user-perception issues.

The literature review confirms that although blockchain is widely seen as a promising enabler of digital transformation in the public sector, it still faces multiple challenges that hinder its diffusion. These challenges span both technical and organizational dimensions and often reinforce one another. For analytical clarity, the main barriers are first presented in descriptive terms and subsequently interpreted from an institutional perspective.

Technical and Operational Barriers

Public administrations struggle to integrate blockchain with existing IT infrastructures due to the absence of shared standards and interoperable protocols, resulting in fragmented data systems rather than seamless inter-agency communication. Scalability remains a persistent limitation, networks such as Bitcoin and Ethereum offer limited throughput and high latency, making them unsuitable for high-volume government applications. Permissioned solutions improve performance but introduce trade-offs in decentralization and security.

Security and privacy issues are also significant. While blockchains ensure data integrity and immutability, their transparency can conflict with public-sector privacy requirements, especially in domains handling sensitive citizen information. Advanced cryptographic methods (e.g. zero-knowledge proofs) are needed to balance confidentiality with auditability. Technological maturity is another concern: smart contracts remain vulnerable, development tools are still evolving, and incidents such as the 2016 DAO hack highlight risks associated with immature systems. Finally, high infrastructure and energy demands - particularly for consensus mechanisms like Proof of Work - pose financial and operational challenges for resource-constrained public agencies. A frequently cited illustration concerns healthcare systems, where fragmented data architectures and strict confidentiality requirements complicate the deployment of distributed ledgers. In such contexts, blockchain initiatives are often motivated by auditability and controlled information sharing across institutional boundaries, yet implementation encounters immediate interoperability constraints and demanding privacy-by-design obligations.

Organizational and Institutional Barriers

Human capital shortages hinder adoption, as few public institutions possess the interdisciplinary expertise needed to manage blockchain projects. This skills gap affects both technical personnel and decision-makers, often increasing reliance on external vendors and limiting internal learning. Cultural resistance within bureaucracies - rooted in established routines, concerns over transparency and accountability, and fears about role displacement - further discourages experimentation.

Regulatory and legal uncertainty compounds these difficulties. Questions persist regarding the official status of blockchain records, compliance with data protection rules such as GDPR, and the lack of recognized standards or certifications. Coordination challenges also emerge in multi-stakeholder environments: blockchain frequently requires cross-agency collaboration, yet governance structures and authority lines are often unclear. Budgetary constraints and uncertain cost-benefit ratios make blockchain appear risky compared with more established digital solutions, especially when short-term value is difficult to demonstrate.

Sector-Specific Variation

The impact of these barriers differs across policy domains. Healthcare emphasizes interoperability and privacy due to fragmented medical records and strict confidentiality requirements. Education focuses on standardization and mutual recognition for credentialing systems. E-government services prioritize legal validity and regulatory compliance. Public finance faces obstacles integrating blockchain with legacy systems and navigating unclear rules for applications such as procurement or budgeting. This heterogeneity indicates that no universal adoption model exists; each sector requires tailored strategies.

Public procurement is frequently highlighted as a high-stakes domain because it combines large spending volumes with complex multi-actor processes and persistent integrity risks. In principle, tamper-evident traceability could strengthen audit trails and reduce opportunities for post hoc manipulation. In practice, however, success depends on governance arrangements (who validates entries, resolves disputes, and updates rules) and on institutional capacity to integrate procurement workflows with digital ledgers without undermining legal due process.

Empirical contextualization further supports this descriptive picture. Evidence from approximately 270 European public-sector blockchain initiatives (JRC, 2022) indicates that most projects remain confined to pilot phases or limited administrative functions, suggesting cautious and experimental deployment. Estonia's national e-health platform is often cited as a rare case of mature implementation. Importantly, its relevance lies less in demonstrating universal applicability than in illustrating how sustained digital capability and established governance routines can enable the integration of blockchain components as integrity-enhancing layers within broader public-service infrastructures.

Interpretive synthesis

Once described in their sectoral and organizational diversity, these barriers can be reinterpreted as manifestations of deeper constraints that shape whether blockchain can function as institutional infrastructure rather than as a stand-alone technical pilot. From this perspective, many “technical” obstacles signal limits in integration capacity, reflecting fragmented legacy architectures, heterogeneous data models, and procurement-driven digitization paths. Likewise, scalability concerns are less about abstract throughput metrics than about the feasibility of embedding distributed systems within mission-critical administrative processes requiring continuity, accountability, and service reliability.

Organizational and regulatory challenges, in turn, point to governance capacity. Blockchain projects typically involve ministries, local authorities, auditors, technology vendors, and sometimes citizens or civil-society actors. Where decision rights over rule modification, system upgrades, or dispute resolution remain unclear, institutional commitment becomes fragile and scaling risks increase. Dependence on external vendors - often a response to skills shortages - may therefore represent not only a short-term resourcing strategy but also a constraint on institutional learning and memory.

Sectoral variation provides an additional diagnostic insight. The fact that barriers manifest differently across domains such as healthcare, procurement, registries, or finance suggests that “blockchain adoption” is better understood as a portfolio of institutional design problems rather than as a single technological transition. Accordingly, successful implementation is likely to depend on sequenced experimentation aligned with sector-specific governance requirements and organizational readiness.

Taken together, the literature supports a central inference for this dissertation: public-sector blockchain adoption is best conceptualized as a constrained institutional design challenge rather than as a conventional process of IT diffusion. Interoperability bottlenecks, regulatory ambiguity, and cultural resistance do not merely slow implementation; they signal that proposed architectures may exceed the current capacity of public organizations to integrate, govern, and sustain socio-technical innovation.

From this standpoint, the institutional relevance of blockchain depends on the ability of public administrations to design governance arrangements, align incentives, and progressively internalize technological competences. The following chapter builds on this diagnostic synthesis by examining whether variations in institutional conditions correlate with observable patterns of blockchain adoption, while subsequent chapters explore how organizational design and incentive structures can translate capability into durable coordination mechanisms.

CHAPTER 2

Blockchain as an Institutional Technology? A Comparative Analysis of Digital Innovation in the European Public Sector

The transition to Chapter 2 marks a shift from conceptual and qualitative insights to a data-driven examination of blockchain adoption. After identifying the main technical and organizational barriers facing public institutions, the thesis moves from synthesizing existing knowledge to presenting original empirical evidence.

Chapter 2 quantitatively analyses how blockchain is diffusing across countries and compares these patterns with the adoption of artificial intelligence (AI) in a large international inventory. This cross-country perspective provides one of the first rigorous tests of the notion that blockchain functions as an “institutional technology” (Davidson et al., 2018), potentially following a diffusion trajectory different from that of more conventional digital technologies.

By drawing on real-world adoption data, the analysis assesses whether the barriers and drivers highlighted in Chapter 1 are reflected in observable global trends and examines the extent to which institutional conditions shape blockchain’s spread. In doing so, the empirical investigation reinforces and contextualizes the earlier findings, linking theoretical insights to measurable adoption dynamics.

2.1 Introduction

Digital innovations are transforming public-sector operations and services across the globe. Technologies such as artificial intelligence (AI) and blockchain have been indicated as drivers of efficiency, transparency, and new service delivery modes in government. Blockchain technology, in particular, has attracted significant attention for its potential to reconfigure institutional processes, for example, by enabling decentralized record-keeping, secure identity management, and automated enforcement of rules via smart contracts.

Early commentators often classified blockchain as a general-purpose technology (GPT), similar to AI, due to its broad applicability across domains (Kane, 2017). However, emerging perspectives suggest that blockchain might fundamentally differ from typical GPTs. Some studies argue that blockchain can be understood as an “institutional technology”, a technology whose core value lies in embedding and automating institutional rules and governance mechanisms (Davidson et al., 2018).

The theoretical literature on technological change provides a useful framework to understand these differences. Following (Dosi, 1982) adaptation of concept of (Kuhn, 1962) scientific paradigm, technological development can be analysed in terms of paradigms and trajectories. A technological paradigm defines the cognitive and technical boundaries that guide engineers’ problem-solving activities, establishing what kinds of questions are legitimate and what

heuristics are available to answer them. Within those boundaries, a technological trajectory, as defined by (Dosi, 1982), describes the cumulative pattern of technical improvements pursued within the boundaries set by a given paradigm. This process often follows a 'challenge-and-response' logic, where engineers progressively refine solutions to practical problems (Rosenberg, 1974). This distinction implies that changes in trajectories correspond to incremental, path-dependent progress, whereas paradigmatic changes reflect discontinuities at the level of knowledge, when prevailing heuristics and problem-solving routines become obsolete and are replaced by new ones (Mokyr, 2005; Vincenti, 1990, 1994).

While much empirical research has focused on trajectories - often by studying improvements in artifacts or generations of products - far less attention has been devoted to paradigmatic change, which occurs at a deeper, knowledge-based level (Anderson & Tushman, 1990; Constant, 1973). As technology historians have shown in domains such as the telecommunications switching industry, innovation dynamics cannot be fully explained by artifact evolution alone. The shift from electro-mechanical to electronic circuit-switching, for instance, was not simply a change in component efficiency but a competence-destroying transformation: it rendered prior engineering heuristics and technical capabilities obsolete, while establishing new cognitive frameworks rooted in semiconductor electronics. Such examples illustrate that paradigmatic shifts redefine the knowledge space of a technology, altering both the problems engineers seek to solve and the institutional structures supporting technological exploration.

This theoretical distinction is essential for interpreting blockchain's evolution. Using (Dosi, 1982) framework, it is possible to ask whether blockchain's development remains confined within the established computational paradigm - driven by heuristics of cryptographic optimization and decentralization - or whether it is moving toward a reorientation of the existing paradigm, where blockchain's evolution becomes progressively shaped by its nature as an institutional technology, that is, by concerns related to institutional design, rule enforcement, and governance functionality rather than purely technical optimisation.

Building on this distinction, first research question investigates whether blockchain's development in the public sector shows signs of strain within the established computational paradigm. In other words, it is explored whether the limited diffusion and uneven performance of blockchain may reflect the mismatch between the prevailing heuristics of the current paradigm - centred on cryptographic optimisation and decentralization - and the institutional coordination problems that governments actually need to solve. Such a misalignment would not by itself demonstrate the existence of a new paradigm, but it would indicate that the established one may be increasingly inadequate for guiding blockchain's evolution in public-sector contexts. The core research questions driving our inquiry are:

RQ1: *Have blockchain's current technological trajectories in the public sector reached a point where the established computational paradigm no longer provides effective heuristics for further development?*

RQ2: *To what extent is blockchain adoption in the European public sector consistent with a framing of blockchain as an institutional technology - relative to AI as a benchmark- rather than with a conventional market-based diffusion pattern within a stable computational paradigm?*

This chapter does not presume an impending paradigmatic rupture. Instead, it empirically tests whether observed adoption correlates are systematically more compatible with an institutional-technology interpretation for blockchain than for AI, given the cross-sectional nature of the available data.

To address these questions, a comparative empirical analysis of blockchain and AI adoption in European public-sector innovation initiatives is conducted. AI is chosen as a comparator because it is a well-established GPT (Allen et al., 2023) and provides a benchmark for “conventional” patterns of technology diffusion. If blockchain truly behaves as an institutional technology, the factors driving its adoption should systematically differ from those driving AI adoption. In particular, based on the theoretical distinction outlined above, one may reasonably expect blockchain uptake to be more closely linked to institutional and governance variables - rather than to market-based innovation inputs - relative to AI. Importantly, this expectation does not imply that such a pattern would automatically validate a paradigmatic reorientation. Rather, it provides a theoretically grounded hypothesis: if blockchain’s diffusion responds to institutional determinants that lie outside the established computational paradigm, and if this response diverges systematically from AI’s, such evidence would be consistent with the idea that blockchain is being engaged by governments through a different problem-framing, one that reflects its potential as an institutional technology. Our empirical analysis is therefore designed to assess whether this theoretical conjecture finds support in observed adoption patterns.

Using an inventory compiled by the European Commission’s Joint Research Centre (JRC) in 2022, which documents 1617 public-sector innovation projects across 32 European countries, the patterns and drivers of adoption for blockchain and AI are compared. The analysis unfolds in two stages. First, an exploratory cluster analysis to categorize countries based on their adoption profiles is performed. This reveals a typology separating “active innovators” – countries with high overall adoption of emerging technologies (especially AI) and strong local government involvement – from “less-active innovators” – countries with more sporadic efforts centered on blockchain and led by central authorities.

Second, a series of negative binomial regression models are estimated to quantitatively assess how various factors (technological capacity, private innovation investment, public-sector size, overall innovativeness, etc.) influence the count of blockchain and AI initiatives in each country. By including interaction terms and comparative specifications, it is probed whether blockchain’s responsiveness to these factors differs significantly from AI’s, and whether cross-technology influences (complementarity or substitution between AI and blockchain) are present.

The findings confirm sharply divergent logics underpinning the adoption of AI and blockchain in the public sector. AI initiatives tend to flourish in environments with strong market-driven innovation (high private R&D spending) and ample public resources, aligning with AI’s

reputation as a flexible, modular technology that can be incrementally integrated into existing systems. In this perspective, AI's development in government aligns closely with this logic: advances in data availability, algorithmic refinement, and computational capacity provide continuous opportunities for performance enhancement without challenging the underlying cognitive and institutional foundations of the prevailing digital paradigm. In this sense, AI behaves as a trajectory within an established paradigm, rather than as a technology whose adoption requires redefinition of problem-spaces or institutional arrangements.

In contrast, blockchain initiatives appear to thrive in contexts with high technological maturity (as reflected by accumulated ICT patents) but not necessarily where private R&D is highest; in fact, we find evidence that very high private R&D may crowd out or substitute for public-sector blockchain projects. Moreover, blockchain projects are disproportionately associated with central government involvement, whereas AI projects are more frequently led by local governments. We also find that when overall innovation activity is low, a country may undertake both AI and blockchain projects in tandem (suggesting a complementary adoption pattern), but in high-innovation contexts, public actors seem to specialize in one technology or the other (indicating a trade-off or competition for resources and attention).

These results provide empirical support for the conceptualization of blockchain as an institutional technology. They suggest that blockchain's value in the public sector is being pursued not primarily for generic computational benefits, but for its potential to embed new governance structures into public administration. This interpretation, however, applies strictly to the public-sector context examined in this study. The data do not allow us to infer whether similar mechanisms operate in other areas of the economy, where blockchain may still follow trajectories consistent with the broader computational paradigm. What results indicate is that, at least within government, blockchain adoption is driven by institutional problem-solving rather than by market-based innovation dynamics. Whether this pattern reflects a broader reorientation of the technology beyond the public domain remains an open question for future research.

In other words, blockchain adoption follows an institutional logic: public agencies engage with blockchain when they seek to reform or enhance institutional processes (especially at the national level), rather than as a side effect of broader innovation trends. AI, on the other hand, fits comfortably within the prevailing computational paradigm, its adoption is more a function of technological opportunity and resource availability, boosting efficiency within existing bureaucratic structures.

By integrating the theoretical perspective with these empirical observations, this work explores whether the evidence is consistent with a potential reorientation in how blockchain is engaged by public institutions, rather than establishing a paradigm shift in blockchain's development. The prevailing blockchain trajectory - dominated by efforts to optimise cryptographic efficiency, decentralisation, and financial applications (e.g., cryptocurrencies, DeFi) - may be approaching diminishing returns within the public-sector domain, where such heuristics often conflict with interoperability requirements, regulatory constraints, and administrative coordination needs. This observation, however, should not be interpreted as evidence of a generalised slowdown of the blockchain trajectory across the entire economy. The data do not

cover private-sector or organisational uses of blockchain, where different incentives, institutional arrangements, and problem-spaces may sustain continued progress within the established computational paradigm. What our findings suggest is more modest but analytically important: in government contexts, the heuristics that have guided blockchain's development in finance and distributed systems appear increasingly misaligned with the institutional challenges public agencies aim to address. Whether similar tensions emerge in private or inter-organisational settings remains an open empirical question, and one that future research should examine before drawing conclusions about broader paradigm-level developments.

The remainder of this chapter is structured as follows. Section 2.2 outlines the theoretical framework. Section 2.3 describes the data and methodology. Section 2.4 presents the results. Section 2.5 provides a discussion of the implications of these findings. Section 2.6 concludes, highlighting the contributions, limitations of the study, and directions for future research.

2.2 Theoretical framework

2.2.1 Technological paradigms and trajectories

The concept of technological paradigms and technological trajectories, as developed by (Dosi, 1982), provides the foundation for this analysis. A technological paradigm can be understood as a model and a pattern for solving selected technological problems, grounded in specific scientific principles and material technologies (Martinelli, 2012). It defines the cognitive boundaries within which engineers identify relevant problems and viable heuristics, thereby shaping the directions in which technological search is pursued. Within these boundaries, a technological trajectory captures the cumulative and path-dependent pattern of improvements that emerges as engineers refine solutions over time. This framework highlights that technological change is not simply the result of linear, continuous progress, but is structured by the problem-solving rules and constraints embedded within each paradigm.

In these paradigms, innovation progresses along technological trajectories, the patterned, cumulative directions of change consistent with the paradigm's guiding heuristics. These trajectories are typically local, cumulative, and path-dependent: once a particular line of problem-solving becomes established, it tends to self-reinforce through specialization, sunk investments, and the institutionalization of expertise. Substantially, trajectories capture a normal problem-solving process, while paradigmatic shifts correspond to the emergence of a new knowledge regime in which both the relevant problems and the acceptable solutions are redefined.

This distinction implies that trajectories are mainly observable at the artifact level, through successive improvements in design or performance, whereas paradigms operate at the knowledge level (Vincenti 1990, 1994; Mokyr 2002). The heuristics embedded in a paradigm represent the cognitive routines and engineering search strategies that guide exploration of the knowledge space. If these heuristics continue to generate meaningful progress, innovation remains within the established paradigm. As suggested by (Constant, 1973), a paradigmatic

shift may occur when a superior alternative paradigm emerges and its effectiveness can be demonstrated. This complements (Rosenberg, 1974) model of ‘challenge-and-response’, which explains how innovation proceeds until existing solutions no longer suffice. Such shifts are typically competence-destroying (Anderson & Tushman, 1990): they render prior technical capabilities and design rules obsolete while establishing new ones around emerging principles. Conceptual insights from (Mokyr, 2005; Vincenti, 1990) help frame this shift in terms of changes in engineering knowledge and technological paradigms. This change fundamentally altered the cognitive and technical heuristics available to engineers, demonstrating how paradigmatic evolution takes place at the knowledge level, while manifesting empirically through discontinuities in artifact generations.

Applied to the present context, the framework motivates an examination of whether blockchain technology is currently situated within a specific paradigm and trajectory, and whether that trajectory exhibits signs of tension in public-sector applications. This consideration is limited to government use cases; the available data do not permit conclusions about private or inter-organisational settings, where the prevailing computational paradigm may continue to provide effective heuristics for further development.

Most of the dominant discourse has situated blockchain within a computational paradigm, emphasizing cryptographic security, decentralization, and performance optimization. The associated trajectory has been guided by heuristics aimed at enhancing technical efficiency - improving consensus algorithms, increasing transaction throughput, and reducing energy consumption - largely in market-driven domains such as cryptocurrencies and decentralized finance (DeFi). These advances represent “normal” technological progress within the prevailing paradigm. Yet, as interoperability challenges, regulatory misalignments, and limited relevance to institutional problem-solving persist, blockchain’s established heuristics may be yielding progressively smaller returns. This tension suggests that, at least within the public-sector context examined, blockchain’s established computational trajectory may be interacting with a different set of institutional problem-solving demands than those for which it was originally optimised. While this does not imply the emergence of a new paradigm, it raises the possibility that blockchain’s development in government is being subtly reoriented by institutional considerations, a possibility further examined in the next section.

2.2.2 Blockchain as an institutional technology

Blockchain technology is often recognized as a General-Purpose Technology (GPT) (Bekar et al., 2018; Kane, 2017) with broad applicability beyond cryptocurrencies. However, an emerging perspective posits that blockchain should instead be viewed as a distinct institutional technology (Davidson et al., 2018). In contrast to typical GPTs (which primarily provide generic computational improvements or cost reductions), an institutional technology embeds rules and governance functions directly into its design. According to (Davidson et al., 2018), blockchains can operate as new institutional infrastructures that transform economic organization. Institutions – understood as the human-devised rules and norms structuring

social and economic interactions – have traditionally been enforced through legal codes, organizational hierarchies, and formal procedures. Blockchain’s distinctive capability is to encode these rules in technological architecture. For example, smart contracts automatically enforce agreements, and distributed ledgers provide trust and transparency without centralized oversight, effectively assuming roles previously played by legal or bureaucratic authorities. In this sense, blockchain offers a form of institutional innovation: it enables new modes of decentralized governance, ensures procedural integrity through tamper-evident records, and automates compliance with regulations via code. Such features “industrialize trust” by shifting it from social or legal institutions into technology protocols (Berg et al., 2017) and signal a new paradigm in which protocol replaces traditional authority. This perspective resonates with a growing strand of e-government research that emphasizes the relevance of governance, legal frameworks, and trust arrangements in blockchain applications, indicating that its potential contribution extends beyond technical improvements to include the reconfiguration of institutional procedures (Davidson et al., 2018).

From the perspective of innovation theory, reframing blockchain as an institutional technology implies a shift in the underlying technological paradigm. Drawing on (Kuhn, 1962)’s concept of paradigms in science and (Dosi, 1982)’s application to technology, a technological paradigm governs the problems engineers focus on and the heuristics used to solve them. Within the prevailing computational paradigm, blockchain development has largely followed normal problem-solving trajectories aimed at improving technical performance, for instance, enhancing cryptographic security, consensus algorithms, throughput, or energy efficiency. Although these developments have generated continuous technical progress, they remain anchored to a cumulative trajectory shaped by the prevailing knowledge base and its objectives, for instance, producing faster or more secure distributed data systems. Indeed, blockchain has been treated like a conventional ICT innovation, and its adoption in government to date has been limited in scope – often confined to pilot projects – with marginal impact on core public-sector systems. This pattern resembles what (Dosi, 1982) would describe as a trajectory approaching its cognitive limits, where further investments in the same heuristic yield diminishing returns. Within the public sector, ongoing challenges related to interoperability, regulatory alignment, and compatibility with administrative requirements suggest that further advances along the existing technical paradigm may be inadequate to address the types of problems governments face. When the central problems of a technology cannot be resolved by existing problem-solving routines, a paradigmatic shift becomes necessary. Such shifts are often competence-destroying, rendering previous expertise and design rules obsolete as new ones arise around different principles.

There are signs that blockchain may be entering such a transition. If blockchain is treated as an institutional rather than purely computational innovation, the guiding heuristics for development would pivot accordingly. The focus would move from maximizing cryptographic efficiency to innovating in institutional design and governance mechanisms and the engineering search heuristics that expand the knowledge base would shift toward questions of organizational fit and rule enforcement. For example, instead of primarily seeking faster consensus algorithms, researchers and practitioners would prioritize solutions like self-

sovereign identity systems, blockchain-based public registries, or smart contract platforms for public procurement – exemplary artifacts of a new paradigm that reconfigure public services and institutional relationships. Within this regime, progress would be measured by improvements in governance outcomes (e.g. transparency, integrity, citizen trust) rather than just technical metrics. This hypothesized reorientation shift mirrors historical cases in which technologies transcended their initial trajectories. Just as the telecommunications industry moved from electromechanical switching to electronic systems by redefining its knowledge base (applying semiconductor electronics to switching, which fundamentally changed design heuristics), blockchain’s advancement may depend on a similar reorientation at the knowledge level. The core proposition is that, in the public-sector context, more substantial progress with blockchain may depend on approaching it as an institutional technology - one whose development is oriented toward governance needs and the creation of public value - rather than solely toward technical refinement. In other words, blockchain’s real promise for government lies in institutional transformation – embedding new rules and trust mechanisms into public infrastructure – rather than in marginal computational improvements. Recognizing this would recast success criteria (focusing on institutional performance and citizen outcomes, not just system throughput) and guide policymakers to support blockchain through legal and organizational innovation, not merely technical experimentation.

2.2.3 Blockchain vs AI: different paradigms and adoption logics

A comparison between blockchain and AI in the public sector highlights their fundamentally different innovation paradigms and adoption logics. AI is widely regarded as a classic GPT (Allen et al., 2023) – similar to electricity or computing – that can be applied modularly across many domains to boost efficiency and decision-making. Its technological paradigm is a mature and relatively stable one: progress in AI has largely come from cumulative improvements in algorithms, models, and data utilization within an established computational framework.

AI development follows a normal trajectory of incremental innovation guided by well-defined heuristics (e.g. improving predictive accuracy, increasing data scale). These advances build on existing computer science knowledge without fundamentally altering the underlying paradigm. In practice, this means AI can be integrated into government operations without necessitating major institutional change. Public-sector AI applications – such as machine learning systems for fraud detection, natural language chatbots for citizen inquiries, or predictive analytics for infrastructure maintenance – are typically introduced as add-ons to enhance existing processes. They tend to optimize decision-making and service delivery within the current organizational rules, rather than rewrite those rules. As a result, jurisdictions with robust digital infrastructure and resources can adopt AI relatively readily: evidence shows that AI uptake in government correlates with a strong innovation ecosystem (e.g. high private R&D investment, ample human capital) and can be achieved through incremental investments in skills and data governance. In short, AI’s public-sector trajectory leverages existing institutional capacity and

amplifies it, a pattern of diffusion consistent with a traditional GPT that thrives in well-resourced, innovation-friendly environments.

Blockchain, on the other hand, appears to follow a divergent logic that may signal an emerging paradigm. Rather than slotting into pre-existing workflows to incrementally improve them, blockchain often demands a rethinking of the workflows themselves and the institutional arrangements behind them. Its evolution in the public sector increasingly involves what might be called institutional heuristics – that is, design strategies aimed at reconfiguring governance, accountability, and trust relationships. This means the problem space for blockchain is defined differently from that of AI. Whereas AI solutions operate within established rules and strive to make better predictions or automate tasks under those rules, blockchain-based solutions frequently seek to encode, modify, or replace the rules of the game by introducing new, built-in mechanisms of coordination. For example, deploying a blockchain for public financial management might involve establishing a tamper-proof ledger of transactions that changes how auditing and oversight are conducted, effectively altering institutional procedures rather than just speeding them up. Consequently, the adoption of blockchain in government tends to hinge on specific institutional motivations – such as a mandate for increased transparency, the need to rebuild trust in public records, or the desire for secure inter-agency data sharing – and often requires adjustments to legal and organizational frameworks. Recent studies underscore this distinction: for instance, (Moura et al., 2020) note that while blockchain promises greater data openness and transparency in public procurement, realizing these benefits necessitates organizational restructuring and new standards (e.g. for data storage and process integration) to fit the public sector’s institutional context. In contrast, AI projects typically can be layered atop existing structures (focusing on data utilization and algorithmic deployment) without fundamentally changing how agencies are organized or how authority is delegated.

External empirical evidence also supports the idea that blockchain and AI follow different public-sector trajectories. For instance, drawing on a cross-country analysis of government innovation initiatives, (Murano et al., 2025) show that blockchain projects are more frequently associated with central administrations and system-wide institutional reforms, whereas AI projects tend to be led by local governments and focus on specific service-level improvements. This evidence provides a benchmark suggesting that the institutional and organizational dynamics we analyse may reflect a broader pattern observed across different public-sector contexts. AI pilots, by contrast, are commonly bottom-up or departmental, like city chatbots or regional AI analytics, which enhance particular functions without overhauling governance structures. This observation dovetails with the finding that blockchain adoption follows an institutional logic: public agencies engage with blockchain primarily when they seek to reform or modernize institutional processes (especially at the national scale), rather than as a side-effect of general technological trends. By comparison, AI adoption aligns with the prevailing computational paradigm, being largely a function of technological opportunity and resource availability within the existing bureaucratic setup. Indeed, (Murano et al., 2025) report that countries strong in traditional innovation inputs (like R&D expenditure) typically showcase high AI activity in government, whereas blockchain activity does not depend on current R&D intensity so much as on a strategic decision to address governance issues in novel ways.

Notably, blockchain projects often emerge when there is an absence of easy alternatives and a pressing institutional need – for instance, combating corruption in public registries or enabling secure multi-party data sharing – which pushes governments to experiment with a new paradigm. This pattern explains why simply having more funding or a vibrant tech sector doesn't automatically lead to blockchain uptake; instead, a conducive regulatory and institutional context is critical. Early case evidence shows that without supportive legal frameworks (for example, recognizing blockchain records as official documents or smart contracts as legally binding) and cross-agency collaboration, many blockchain projects stall despite their technical viability. By contrast, AI implementations mainly raise issues of data privacy, ethics, and scaling of algorithms – important challenges, but ones that can often be managed within existing policy regimes (such as data protection laws and procurement of IT services), rather than requiring entirely new institutional structures.

Thus, AI and blockchain could represent two distinct innovation paradigms in the public sector. AI extends a stable paradigm of data-centric, computational improvement that integrates into current bureaucratic processes, often enhancing efficiency without demanding structural change. Blockchain, in emerging as an institutional technology, signals a potential paradigm shift wherein technological innovation and institutional reform go hand in hand. Its adoption is governed by a different logic – one that looks beyond automating tasks to redesigning the rules and trust mechanisms underlying public services. This contrast has practical implications: governments can treat AI as a powerful tool within the status quo model of public administration, but harnessing blockchain effectively may require a reconfiguration of that model. Thus, while both technologies are often mentioned in the same breath as drivers of digital transformation, their routes into government and their demands on public organizations diverge significantly. Recognizing this divergence is essential for policymakers and scholars alike, as it emphasizes that technology adoption is not monolithic: the institutional context and purpose of a technology must be considered. In the case of blockchain, its success in the public realm likely depends on aligning technological deployment with institutional change, a theme that will be further reflected in the conclusions and recommendations for public governance and policy.

2.3 Data and Methodology

2.3.1 Data source and scope

The empirical analysis utilizes an inventory of public-sector technology innovation initiatives compiled by the European Commission (CEU, JRC 2022). This inventory catalogues a wide range of digital innovation projects in the public sectors of European countries. Each observation in the inventory corresponds to a specific initiative and includes information on: the technology or technologies employed (with a focus on AI and blockchain, but also covering some cases of other emerging tech like augmented/virtual reality, albeit the latter represent less than 3% of initiatives), the sector or policy domain of application (e.g., health, transportation, general public services, economic affairs, etc.), the implementing agency level

(central/federal government vs. local/regional authority), the implementation status (pilot, deployed, etc.), and various country-level contextual variables. In total, the inventory contains 1617 initiatives across what were initially 42 geographic entities (EU member states, associated countries, plus EU-level programs). For consistency with available country-level covariates, the focus is on 32 countries for which complete data on innovation environment indicators are available (essentially EU-27 plus a few additional European countries included in the inventory).

It is important to note a limitation of the data: the inventory is based on identified initiatives found through online sources and reports, and while extensive, it may not be exhaustive. Some projects might be underreported or omitted. Thus, the data provide a valuable but possibly incomplete picture of technology adoption in the public sector. Nonetheless, this is one of the most comprehensive collections of such initiatives to date, and it offers a useful starting point for analysing broad patterns and drivers of adoption.

2.3.2 Exploratory analysis: clustering countries by adoption patterns

Before delving into causal drivers, an exploratory analysis is performed to see if countries cluster into meaningful groups based on their adoption of AI and blockchain in the public sector. Principal Component Analysis (PCA) is used, followed by cluster analysis on country-level summary metrics of the initiatives. Specifically, for each country we compute measures such as the total number of initiatives, the share of initiatives involving AI, the share involving blockchain, the distribution of initiatives across sectors, and the distribution by government level (central vs. local). Using these features, PCA is applied to reduce dimensionality and identify principal components that capture the most variance in adoption patterns. The PCA considers key categories of variables: technology usage (AI vs blockchain prevalence), application sectors, and implementing organizational level. We then apply a clustering algorithm (here a hierarchical clustering, though k-means yields similar groupings) on the principal component scores to group countries with similar profiles. This procedure yields a clear bifurcation into two clusters of countries, primarily distinguished by their overall level of activity in tech innovation and the type of technology emphasized:

- i. *Cluster 1, “Active Innovators”*. This cluster comprises countries with a high volume of public-sector innovation initiatives (per country) and a focus on AI. These countries tend to have strong local government involvement in projects and a significant portion of initiatives in forward-looking sectors (for instance, projects geared toward economic affairs, industrial policy, or “smart city” initiatives). In these countries, AI appears as the predominant technology for public innovation, suggesting an orientation toward technologies with high systemic applicability and maturity. The decentralized nature of their innovation (many local-level projects) implies a bottom-up experimentation culture.

- ii. *Cluster 2, “Less-Active (Emergent) Innovators”*. This group includes countries with fewer recorded initiatives, where blockchain projects make up a larger share of their activities. Here, we see a relative emphasis on general public services (including foundational government functions like identity management, land registries, public records) and a greater role of central government in driving projects. These countries’ innovation efforts, while fewer, are often top-down and focused on traditional state functions. The prominence of blockchain in these contexts may indicate targeted efforts to modernize specific institutional functions, albeit not yet at a systemic scale.

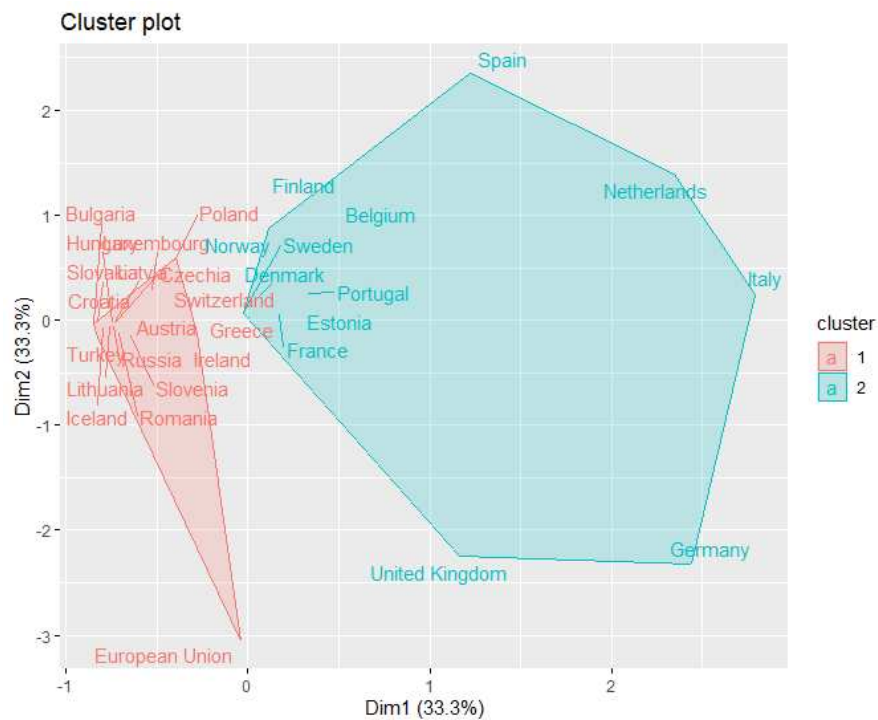


Figure 1 - Country clusters based on technological adoption patterns.

The cluster analysis thus provides an initial indication that more active innovators lean heavily on AI and local experimentation, whereas less-active innovators, though engaging more with blockchain, do so in a narrower, centralized manner. This descriptive finding foreshadows the regression results: it hints at different driving forces behind AI and blockchain uptake, aligning with the idea that blockchain might be pursued for specific institutional purposes especially in environments where broad-based innovation activity is lower.

2.3.3 Econometric strategy

To rigorously assess the determinants of technology adoption, count data regression models for the number of initiatives in each country are employed. Since the dependent variables are counts of initiatives (which are non-negative integers) and in data these counts exhibit over-dispersion (variance exceeding the mean), a Negative Binomial regression approach is

appropriate. Different models for different dependent variables to compare drivers are estimate:

All: Total number of initiatives per country.

Bcs: Number of blockchain-specific initiatives.

Ais: Number of AI-specific initiatives.

Each regression takes the general form:

$$\text{Initiatives}_i = \alpha + \beta_1 \text{ICTpatents}_i + \beta_2 \text{R\&D}_i + \beta_3 \text{PAexpense}_i + \mu_{i,t} \quad (1)$$

where the key explanatory variables are defined as follows:

- i. *ICTpatents*. A proxy for the country's accumulated technological maturity, measured as the stock of ICT-related patents (e.g., patent applications in ICT fields). This variable captures the knowledge base and innovative output of the private sector that could spill over to public innovation.
- ii. *R&D*. Private Research & Development expenditure (business R&D spending as a percentage of GDP). This gauges the intensity of market-driven innovation efforts in the country, representing the resources and attention the private sector dedicates to developing new technologies.
- iii. *PAexpense*. Public Administration expenditure (government spending on public administration as a share of GDP, or per capita). This reflects the size and resource capacity of the public sector, indicating how much funding is available for public agencies and potentially for innovation within government.

For all variables employed in the estimations, descriptive statistics are reported in the following table.

Table 1 – Descriptive statistics

iv.

<i>Variable</i>	<i>Description</i>	<i>Source</i>	<i>Sd</i>	<i>Mean</i>
<i>ais</i>	Number of initiatives related to Artificial Intelligence	PSTW, JRC 2022	45.97	40.00
<i>bcs</i>	Number of initiatives related to Blockchain	PSTW, JRC 2022	11.47	7.9
<i>all</i>	Number of initiatives related to Artificial Intelligence and Blockchain	PSTW, JRC 2022	56.19	49.53
<i>ICTpatents</i>	ICT patent application EPO – avg 2014-2021 (log)	OECD STAT	2.25	4.36
<i>R&D</i>	Business Enterprise Expenditure on R&D – avg 2014-2023 (log)	OECD STAT	0.63	-0.03
<i>PAexpense</i>	payments of the government in providing goods and services – avg 2008-2022 (log of % of GDP)	World Bank	0.20	3.60

The analysis begins with a baseline specification (Models 1–3) that includes these core variables for each dependent variable category without any additional interaction or control terms. These baseline regressions allow us to see the fundamental relationships between a country’s innovation environment and its public-sector adoption of new technologies:

Model 1: Dependent variable = All initiatives (total count in country)

Model 2: Dependent variable = Blockchain initiatives (Bcs count)

Model 3: Dependent variable = AI initiatives (Ais count)

Each model has its own intercept α , and error term μ_i to capture unobserved country-specific factors. The coefficients $\beta_1, \beta_2, \beta_3$ on the main explanatory variables can be compared across the models to discern differences in drivers between blockchain and AI.

Next, the models are extended in two ways to delve deeper into interaction effects and latent factors:

1. *Cross-technology controls and interaction terms.* Each technology’s “counterpart” is introduced as a regressor to test for complementarity or substitution effects, and interaction terms are added to explore how the effect of one variable may depend on the level of another. For instance, in the blockchain equation the count of AI initiatives (Ais_i) is included as an additional regressor, and vice versa, to see if having more of one technology’s projects is associated with more of the other (complementarity) or fewer (substitution). Interactions like $ICTpatents \times Ais$ or $R\&D \times Ais$ are tested in the blockchain equation (and analogous $\times Bcs$ in the AI equation) to examine whether the presence of one technology moderates the effect of innovation inputs on the other’s adoption. The inclusion of these terms is motivated by the hypothesis that, for example, a highly innovative environment might either encourage using multiple technologies together or foster competition where one dominates.
2. *Cluster dummy variable.* To capture the broad differences identified in the exploratory clustering (active vs less-active innovators), a binary dummy variable is included for the country being in the “Active innovator” cluster. This variable equals 1 for countries in Cluster 1 (high overall adoption, AI-focused) and 0 for those in Cluster 2 (lower adoption, blockchain-skewed). By adding this to the regression (referred to as the Extended Models), the specification accounts for unobserved institutional or policy factors that differentiate the two clusters, effectively a latent profile of the country’s innovation ecosystem that might not be fully captured by quantitative variables. Prior to its inclusion, it was verified that the variable is not simply a proxy for the other explanatory factors (a logistic regression predicting cluster membership from the

innovation variables showed no significant dependency, indicating the cluster captures additional characteristics).

The extended models are estimated in a stepwise manner: first incorporating cross-technology terms, then interaction terms, and finally the cluster dummy, allowing observation of how model fit, and coefficient patterns evolve. Goodness-of-fit measures are reported, including the Akaike Information Criterion (AIC) for model comparison and pseudo- R^2 measures (McFadden's R^2 and Maximum Likelihood pseudo- R^2 to assess explanatory power. Statistical significance tests are conducted to identify which factors exert a robust influence on each type of initiative.

All estimations are based on a cross-section of 32 countries. Given the relatively small sample size, the findings are interpreted cautiously and regarded as exploratory. Emphasis is placed on the direction and significance of coefficients - specifically, whether they correspond to the hypothesized differences between blockchain and AI adoption drivers - rather than on precise point estimates.

2.4 Results

2.4.1 Country clusters: Active vs. Less-Active innovators

The clustering analysis uncovers a pronounced split in how European countries approach public-sector digital innovation. Figure 1 (referenced above) visualized this division. Here the key characteristics of the two clusters are summarized:

Cluster 1, “Active Innovators”. This group (comprising roughly 13 of the 32 countries) shows a high total count of initiatives. These countries' public sectors are broadly engaged in digital innovation, often experimenting with multiple technologies. A defining feature is the prevalence of AI projects: AI is used in a wide array of pilots and implementations, indicating it is currently the technology of choice for many public-sector innovation efforts. The initiatives in these countries commonly address areas categorized under economic affairs or similar domains related to economic development and public sector modernization (suggesting effective industrial and innovation policies might be in place). Moreover, a larger share of projects in these countries is driven by local governments or municipalities, reflecting a decentralized or bottom-up approach to innovation. This could imply that in these environments, cities and regions have the autonomy and capacity to implement AI solutions for local governance challenges (smart city applications, local e-government services, etc.).

Cluster 2, “Less-Active (Selective) Innovators”. The remaining countries (approximately 19 out of 32) form a cluster characterized by lower overall counts of initiatives. Importantly, a lower observed initiative count in a cross-sectional snapshot can reflect not only limited current

experimentation, but also a degree of prior ICT and e-government capability accumulation that reduces the need for numerous “new” pilots while enabling more selective experimentation (e.g., in core administrative domains). What stands out in this cluster is that, within their more limited activity, blockchain projects comprise a relatively significant portion. In other words, these countries are not at the forefront of public-sector innovation in terms of volume, but when they do innovate, they lean somewhat more towards blockchain use-cases. Their projects often concentrate on general public services, core administrative functions such as registries (land, business, or civil registries), identity management systems, voting or recordkeeping platforms, etc. These are areas where blockchain’s properties (secure, tamper-proof transactions and records) could be directly applied to enhance trust and integrity. Additionally, in this cluster a top-down dynamic is evident: central governments play a leading role in initiating and executing projects, as opposed to the local-level dynamism seen in Cluster 1. This may reflect a more cautious or controlled approach to innovation, possibly due to more centralized governance structures or fewer resources to diffuse to local experimentation. The picture that emerges is one of targeted modernization of traditional state functions (often via blockchain pilots), rather than broad-based digital transformation.

This pattern is empirically confirmed by the distribution of blockchain initiatives across policy domains. As shown in Figure 2, the vast majority of blockchain projects are concentrated in “General public services” and, to a lesser extent, “Economic affairs”. These are core state functions directly associated with identity management, registries, and administrative control, consistent with the hypothesis that blockchain serves institutional, rather than purely technological, purposes.

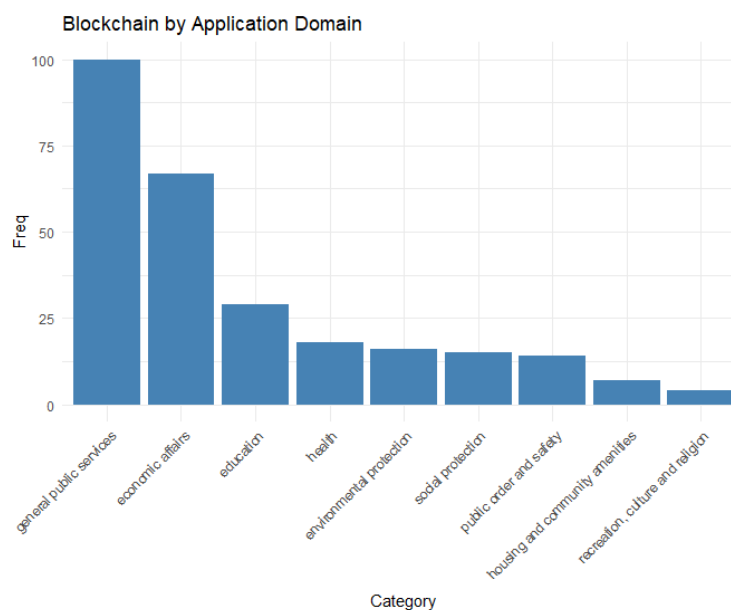


Figure 2 - Blockchain by application domain

Furthermore, the institutional nature of blockchain adoption is reflected in the identity of the leading actors. As reported in Figure 3, central government authorities are the primary promoters of blockchain initiatives, while local governments dominate AI-related projects.

This reinforces the interpretation that blockchain is deployed to redesign foundational state infrastructures rather than to deliver incremental service improvements.

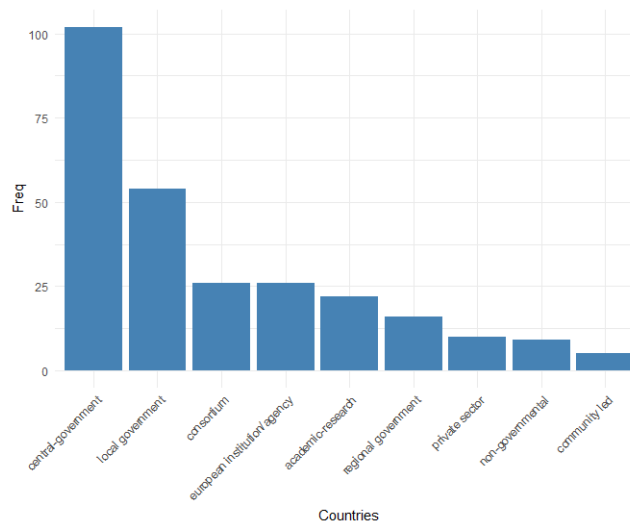


Figure 3 - Lead actor / organization type

Moreover, Figure 4 shows that over 60 percent of blockchain initiatives remain in the pilot stage, indicating an early phase of paradigm exploration rather than consolidation.

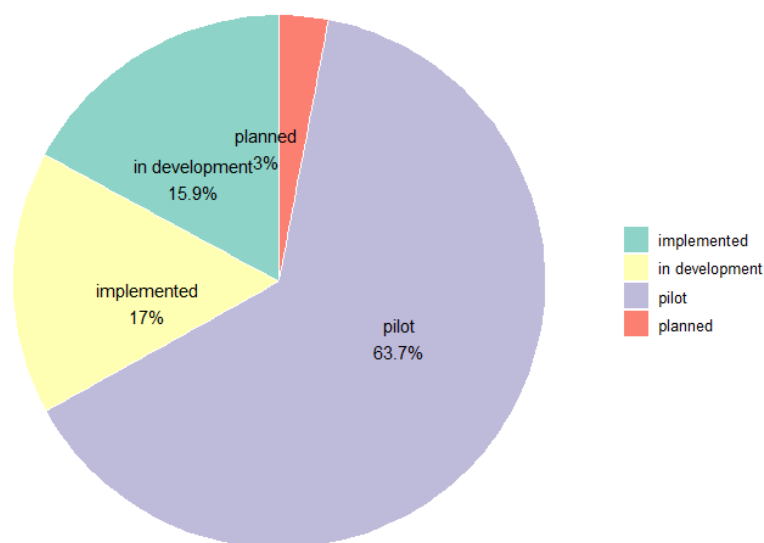


Figure 4 - Implementation status

These clusters provide contextual background for the regression analysis: they suggest that any modelling of adoption drivers should account for the fact that countries with high innovation activity differ qualitatively (not just quantitatively) from those with lower activity. The inclusion of the cluster dummy in later models will help capture these differences. Next, we turn to the regression results for a more formal analysis of adoption drivers.

As further illustrated in Figure 1, the distribution of blockchain initiatives across countries is highly skewed, with a small number of early adopters accounting for the majority of projects. This overdispersion provides a strong econometric justification for modelling the count of initiatives using a Negative Binomial specification rather than a standard Poisson model.

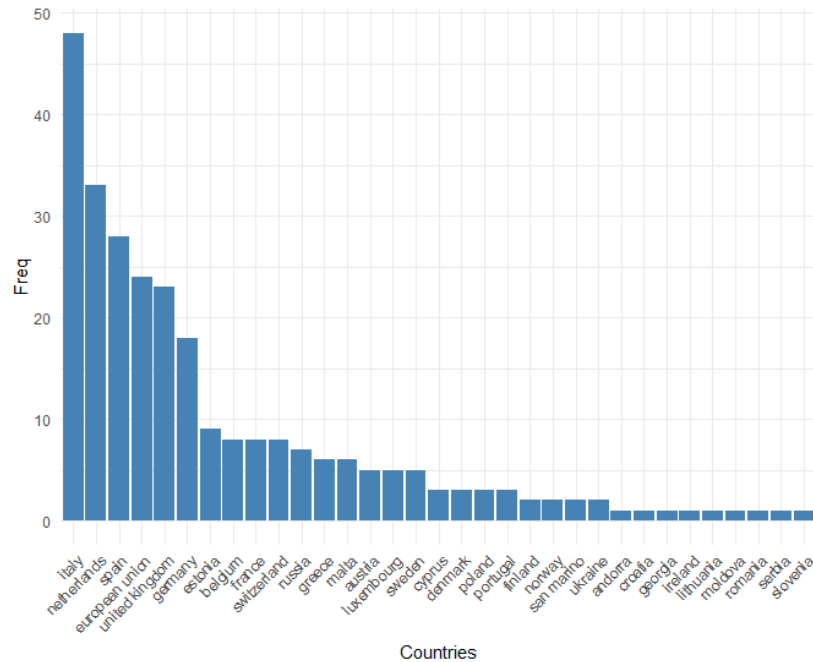


Figure 5 - Blockchain initiatives by country

2.4.2 Baseline regression results

The baseline negative binomial regressions (Table 2) analyse how country-level innovation factors correlate with the number of public-sector initiatives, under three scenarios: total initiatives (All), blockchain initiatives (Bcs), and AI initiatives (Ais).

Table 2 below presents the estimated coefficients. Each column corresponds to a dependent variable (All, Bcs, Ais). Coefficients for Intercept, ICTpatents, R&D, and PAexpense are listed, with significance levels indicated.

	Model 1	Model 2	Model 3
Intercept	-3.9680	-3.8082	-5.0173
ICTpatents	0.3738***	0.6070***	0.3251***
R&D	0.1523	-0.6184	0.3015
PAexpense	1.6434***	0.7461	1.9420***
AIC	303.04	182.96	292.48
McFadden's R²	0.064	0.107	0.051
ML pseudo R²	0.467	0.476	0.379

Note: *** $p < 0.01$, ** $p < 0.05$, * $p < 0.10$

Table 2. Baseline Regression Results (No Interaction Terms).

Several important observations emerge from these baseline models.

ICT Patent Stock is a strong positive predictor in all three models and is statistically significant at the 1% level throughout. This suggests that countries with a more mature technological innovation base (accumulated ICT knowledge as evidenced by patent output) tend to have more public-sector digital initiatives of all kinds. Because ICTpatents is a stock-like measure, a plausible complementary interpretation is explicitly path-dependent: it may proxy the accumulated ICT trajectory of a country, including long-run experience with earlier waves of digital government and e-government capability building. The effect is notably largest for blockchain initiatives ($\beta \approx 0.61$ in Model 2, compared to 0.37 for All initiatives and 0.33 for AI). This pattern is consistent with the idea that administrations with deeper accumulated ICT capabilities may be better positioned (and institutionally motivated) to explore blockchain in domains where integrity, registries, and inter-agency coordination are salient, whereas AI diffusion may be more strongly associated with frontier-oriented innovation dynamics in the present. Given the cross-sectional design, this remains an interpretive reading consistent with observed correlations rather than a causal time-dynamic claim.

Private R&D Expenditure shows no statistically robust association at conventional levels in these baseline specifications, and differences in sign across models should therefore not be over-interpreted in the baseline setting. Accordingly, the discussion prioritizes coefficients that are stable and statistically supported, while the extended models (Tables 2–3) are used to explore whether cross-technology linkages and interaction effects emerge once additional structure is introduced.

Public Administration Expenditure (PAexpense) is positive and significant for All initiatives and AI initiatives (Models 1 and 3), but positive and not significant for blockchain (Model 2). The coefficient for PAexpense in Model 1 (≈ 1.64) and Model 3 (≈ 1.94) are both significant at 1%, indicating that countries which invest more in their public sector (higher government spending on administration) tend to undertake more digital innovation projects in general, and especially more AI projects. This makes intuitive sense: a well-funded public sector has greater capacity to invest in new technologies, and AI projects often require ongoing resources (for data management, procurement of AI systems, hiring data scientists, etc.). However, the lack of significance for blockchain projects suggests that simply having a larger or better-funded public sector is not a guaranteed driver for blockchain. Blockchain initiatives might depend more on specific strategic decisions or needs (which are not captured by aggregate spending alone) rather than on the sheer availability of funds.

In terms of overall fit, Model 2 (blockchain) interestingly shows the lowest AIC and highest pseudo- R^2 among the three, despite having fewer observations (because blockchain initiatives are fewer than AI initiatives). This implies that the included variables explain the variation in blockchain counts relatively well compared to AI. In particular, the much lower AIC for Model

2 (182.96) vs Model 3 (292.48) suggests a better model fit for blockchain. One might interpret this as an indication that blockchain adoption, while less common, follows a more specific pattern that these variables (especially ICT patents and R&D) capture to a significant extent, whereas AI adoption may be influenced by a broader array of factors or inherent variability not fully captured here.

To summarize the baseline findings is possible to note that technological maturity (patent stock) consistently drives both blockchain and AI adoption, underscoring the importance of a strong knowledge and innovation ecosystem. However, private R&D effort and public spending have asymmetric effects: they are aligned with AI uptake but not with blockchain. This provides a first clue that blockchain's adoption logic diverges – being in a high R&D, well-funded environment guarantees AI projects, but not necessarily blockchain projects.

2.4.3 Extended Regression Results: Interaction Effects and Cluster Factor

In this section the analysis turns to the extended models that incorporate cross-technology influences and interaction terms (Table 2), as well as the models that include the cluster dummy (Table 3). These results will help unravel whether AI and blockchain act as complements or substitutes in public-sector innovation, and how the innovation context moderates their relationship.

Table 3. Regression Results with Cross-Technology Controls and Interaction Terms. This table will be split into two panels for clarity:

Panel A: Dependent Variable = Blockchain Initiatives (Bcs)

Panel B: Dependent Variable = AI Initiatives (Ais)

Each panel will have multiple columns (models) showing incremental additions of terms. For example, Model A1 might include the other tech count (Ais in the Bcs equation) as a regressor, Model A2 adds one interaction, Model A3 adds another, etc. Similarly for Panel B.

Panel A – Dependent Variable: Bcs (Blockchain count)

	Model 1	Model 2	Model 3	Model 4
Intercept	-0.5296	-0.3671	-0.9009	1.5417
ICTpatents	0.4350***	0.4430***	0.5948***	0.4296***

	Model 1	Model 2	Model 3	Model 4
R&D	-0.6251*	-0.0558	-0.6821**	-0.6170*
PAexpense	-0.1469	-0.2023	-0.2943	-0.71768
Ais	0.0138***	0.0168***	0.0444***	-0.06618
ICTpatents × Ais	–	–	-0.0050**	-
R&D × Ais	–	-0.0183**	–	-
PAexpense x Ais	-	-	-	0.0220
AIC	173.62	167.67	168.97	174.3
McFadden's R²	0.165	0.206	0.199	0.172
ML pseudo R²	0.632	0.713	0.701	0.647

N (countries) = 32

Panel B – Dependent Variable: Ais (AI count)

	Model 1	Model 2	Model 3	Model 4
Intercept	-3.1003	-7.0303*	-3.8392	-3.0991
ICTpatents	0.1071	0.0783	0.2968**	0.1077
R&D	0.6613*	0.6831**	0.4885	0.6625*
PAexpense	1.5577*	2.6545**	1.5362**	1.5568*
Bcs	0.0443*	0.6062	0.1836***	0.0443**
ICTpatents × Bcs	-	-	-0.0241**	-
PAexpense × Bcs	-	-0.1520	-	-
R&D x Bcs	-	-	-	-0.0005
AIC	288.73	288.66	286.96	290.73
McFadden's R²	0.070	0.077	0.083	0.070
ML pseudo R²	0.481	0.514	0.539	0.481

N (countries) = 32

| *Note: Significance levels as before. Interaction terms introduced sequentially: for Bcs models, Model A2 adds R&D×Ais, Model A3 adds ICTpatents×Ais; for Ais models, Model B2 adds PAexpense×Bcs, Model B3 adds ICTpatents×Bcs (while possibly dropping an insignificant interaction for parsimony). |*

Panels A and B are reported with symmetric candidate interaction terms. In particular, if $PA_{expense} \times BCs$ is included in Panel B, the corresponding $PA_{expense} \times Ais$ term is included (or explicitly marked as omitted) in Panel A; likewise, if $R\&D \times Ais$ is included in Panel A, the corresponding $R\&D \times BCs$ term is included (or explicitly marked as omitted) in Panel B.

Key findings from Table 3

In the Blockchain equation (Panel A), the inclusion of Ais (AI initiative count) as a regressor (Model A1) is significant and positive. The coefficient ~ 0.014 (and increasing in later models) implies that, holding other factors constant, countries with more AI projects also tend to have more blockchain projects. This initial result indicates a complementarity: some underlying propensity leads countries to pursue both technologies. It aligns with the earlier notion that low-innovation contexts might use whatever opportunities available, doing a bit of both AI and blockchain. The model fit improves substantially with this addition (compare AIC of 173.62 in Model A1 with 182.96 in baseline Model 2), and McFadden's R^2 jumps from ~ 0.11 to ~ 0.165 , suggesting that accounting for AI activity provides additional explanatory power for blockchain counts.

However, when interaction terms are added, a more nuanced story emerges. In Model A2, an interaction between $R\&D$ and Ais is introduced. The $R\&D \times Ais$ term is negative and statistically significant, while the main effect of $R\&D$ becomes nearly zero (and insignificant). What this means is that the effect of private $R\&D$ on blockchain adoption depends on the level of AI activity: when AI initiatives are zero (which is rare, only one country has no AI projects at all), the model suggests $R\&D$'s effect on blockchain is not significant. But as AI initiatives increase, the negative interaction indicates that in countries with higher $R\&D$, the positive association between AI and blockchain adoption weakens. In other words, private $R\&D$ moderates the complementarity between AI and blockchain: if private $R\&D$ is low, a rise in AI projects strongly accompanies a rise in blockchain projects (possibly because public sector is filling an innovation void by trying both). But if private $R\&D$ is high, an increase in AI projects yields a smaller increase (or eventually a decrease) in blockchain projects, hinting at a competitive or substitutive effect in high-innovation contexts.

In Model A3, the $R\&D \times Ais$ interaction (which in Model A3 of the table seems to be dropped, and instead we add $ICTpatents \times Ais$) is removed. The $ICTpatents \times Ais$ interaction comes in negative and significant. Here, both $ICTpatents$ and Ais on their own are positive contributors to blockchain count, but their product term having a negative coefficient suggests a diminishing returns or trade-off effect: at very high levels of technological maturity (lots of ICT patents) combined with a high number of AI projects, the expected blockchain count is lower than it would be if the effects were purely additive. Substantively, this implies that in the most technologically advanced countries that are also doing a lot of AI in government, blockchain initiatives might be relatively fewer – possibly because those environments channel innovation efforts preferentially into AI (the technology with more readily attainable benefits), or because the presence of many AI projects means the problems that could be solved by digital tech are being addressed by AI already, leaving less niche or urgency for blockchain solutions. Notably, the main effect of $ICTpatents$ remains strongly positive throughout, reaffirming its general

importance for blockchain capacity; this interaction just tempers that effect when AI is also high.

Throughout the Panel A models, PAexpense remains insignificant for blockchain, and its coefficient even turns slightly negative when interactions are added (though not significant). This reinforces the earlier conclusion that a large public budget alone is not a driver for blockchain projects. Blockchain appears more demand-driven by specific needs or enabled by knowledge factors, rather than by general public sector spending.

Turning to the AI equation (Panel B), it is possible to see a mirror image in some respects. Including Bcs (blockchain count) as a regressor in Model B1 yields a small positive coefficient (~ 0.044 , significant at 10%). This indicates a baseline complementarity: countries with more blockchain projects tend to have slightly more AI projects, controlling for other factors. However, the effect is weaker than the converse (AI on blockchain), consistent with the idea that AI is the dominant, more widespread tech – it exists in many countries regardless of blockchain, whereas blockchain rarely appears without some AI presence. The inclusion of Bcs improves the AI model fit marginally (McFadden's R^2 rises from ~ 0.051 to ~ 0.070 , and AIC drops a bit), so there is some informational value in knowing blockchain count for predicting AI count. In Model B2, adding an interaction $PAexpense \times Bcs$ tests whether the impact of public sector size on AI adoption changes with blockchain presence. The interaction here is negative but not significant (as shown, it is included but it does not reach significance and might be dropped later). Its negative sign might intuitively suggest that if a country is doing blockchain projects, the marginal return of more public spending on adding AI projects is less – possibly because resources get diverted or because a focus on blockchain by central authorities might detract from AI diffusion. However, since it's not significant, we don't over-interpret this. What is noticeable is that in Model B2, the coefficients on ICTpatents, R&D, and PAexpense all increase in magnitude and become significant (R&D and PAexpense become significant at 5%). This could indicate that when accounting for whether a country is doing blockchain, the remaining variance in AI adoption is explained even more by these innovation inputs; or put differently, among countries with similar blockchain activity, those with higher R&D and PA spending do more AI. It underscores that AI adoption responds strongly to both private and public sector inputs.

In Model B3, the $ICTpatents \times Bcs$ interaction is added (and the insignificant $PAexpense \times Bcs$ dropped). Here we find an interesting parallel to the blockchain case: the interaction is negative and significant, while the main effects of ICTpatents and Bcs are positive. This mirrors the notion of a moderating effect of technological maturity on joint adoption: at very high levels of ICTpatenting, if a country also has many blockchain projects, the AI project count is somewhat lower than expected from each factor alone. In other words, extremely tech-mature countries seem to specialize: if they have a strong blockchain program in the public sector, they might not push AI as much, given both are advanced technologies vying for attention/resources. Meanwhile, in less tech-mature countries, doing blockchain and AI together might still be complementary (as indicated by the positive main effect of Bcs, which is larger when not offset by the interaction in lower patent contexts).

Summarizing the interaction results, there is evidence of both complementarity and substitution between AI and blockchain adoption, contingent on the innovation context. In countries with lower levels of R&D and technological maturity, blockchain and AI adoptions tend to go hand-in-hand (complementary) – possibly as part of a general drive to modernize that embraces any available technology. However, in high-R&D or high-patent environments, we observe signs of a trade-off – a sort of crowding-out where extensive activity in one technology is associated with relatively less of the other. This trade-off is consistent with the idea that public agencies face resource constraints and strategic choices: advanced countries might evaluate where to invest marginal effort and could determine that AI yields more immediate returns, thereby de-emphasizing blockchain (or vice versa in a niche case).

It's also notable how the sign of the R&D coefficient flips between the blockchain and AI models. In the blockchain models, R&D tends negative (significantly so in some specifications), indicating a possible crowding-out effect: high private R&D may absorb talent, focus, and incentives in the private sector such that the public sector's direct adoption of a complex new technology like blockchain is hindered. The narrative from the detailed analysis in our data is: private firms heavily investing in R&D might be drawing upon the same pool of skilled workers or might be delivering solutions themselves, leading governments in those contexts to either rely on private solutions (thus fewer independent blockchain projects by the government) or to see less urgency in stepping in with their own projects. On the other hand, in AI models, R&D is a positive force, reflecting spillovers or collaboration – private sector AI development makes tools and expertise available that the public sector can readily apply (especially since many AI solutions are offered as commercial off-the-shelf or cloud services). Finally, the cluster dummy variable is included into the regression to capture the broad active vs. less-active country differences.

Table 4. Extended Models with Cluster Dummy Variable.

This table will show two columns for each dependent variable: without cluster vs with cluster. For brevity, only the cluster dummy's effect and changes in other coefficients are highlighted.

	All (no cluster)	All (+ cluster)	Bcs (no cluster)	Bcs (+ cluster)	Ais (no cluster)	Ais (+ cluster)
Intercept	-3.9680	0.2407	-3.8082	-1.3874	-5.0173	-0.0146
ICTpatents	0.3738***	0.2213***	0.6070***	0.5062***	0.3251***	0.1329**
R&D	0.1523	-0.1609	-0.6184	-0.7457*	0.3015	-0.0495
PAexpense	1.6434***	0.3978	0.7461	0.0402	1.9420***	0.4826
Cluster (Active=1)	–	1.7013***	–	1.0964***	–	1.9414***
AIC	303.04	273.73	182.96	177.91	292.48	265.18
McFadden's R ²	0.064	0.164	0.107	0.143	0.051	0.149

	All (no cluster)	All (+ cluster)	Bcs (no cluster)	Bcs (+ cluster)	Ais (no cluster)	Ais (+ cluster)
ML pseudo R ²	0.467	0.799	0.476	0.579	0.379	0.751

*** p<0.01, ** p<0.05, * p<0.10

In all cases, the cluster dummy is positive and highly significant. This indicates that, even after controlling for the specific innovation inputs (patents, R&D, spending), being an “active innovator” country (Cluster 1) is associated with substantially more initiatives of all types. The coefficient is largest for AI initiatives (nearly 1.94), which makes sense since the cluster essentially was defined partly by high AI activity. But interestingly, it is also positive and significant for blockchain count (~1.10), implying that active innovator countries, despite favouring AI, also tend to have more blockchain projects than the less-active ones. In other words, the cluster captures a general innovation-friendly institutional environment – perhaps related to unobserved factors like national digital strategy, innovation culture in the public sector, or regional innovation funds – that boosts both AI and blockchain adoption beyond what raw R&D and budget numbers would predict.

Including the cluster variable also improves model fit markedly (AIC drops and pseudo-R² jumps in each case, especially for total initiatives where pseudo-R² goes from 0.467 to 0.799, indicating a huge share of variance explained by simply knowing the cluster). This underscores that the binary distinction between high-innovation and low-innovation contexts is a critical piece of understanding the adoption patterns.

Notably, when cluster is included, some coefficients on other variables change: for example, R&D becomes negatively signed in all equations (significant for blockchain). This suggests that some of what was previously attributed to R&D (or PAexpense) was actually the effect of being in the high-innovation cluster. It appears that cluster membership subsumes a lot of the positive effect of general public spending on adoption; once you know a country is in the active cluster, the raw spending level matters less, consistent with the interpretation that it’s not just money, but how it’s used and the institutional context that drives innovation. Similarly, ICTpatents remains significant but its coefficient is reduced when cluster is present, implying that tech maturity still matters within clusters, but part of its effect was correlated with being an active innovator country.

2.4.4 Summary of Empirical Findings

Bringing together all results, several robust patterns emerge.

The stock of ICT patents is a consistently positive driver for both blockchain and AI adoption. Countries with mature innovation ecosystems have a higher propensity to implement new technologies in the public sector. This likely reflects the availability of technology providers and expertise, as well as a culture of innovation that spills over into public governance.

Private R&D expenditure shows a divergent relationship: it is neutral-to-positive for AI adoption but tends to be negative for blockchain adoption. High private R&D could indicate that the private sector is actively absorbing technological opportunities (perhaps leaving the public sector in a follower position). For AI, this dynamic is synergistic, public agencies can piggyback on advances made by private firms (for instance, adopting AI tools developed by tech companies). For blockchain, however, heavy private sector focus (e.g., fintech companies or tech giants investing in blockchain R&D) might reduce the necessity or capability of public agencies to engage directly (they may either rely on private solutions or face competition for skilled personnel). In sum, blockchain appears more institutionally driven, flourishing in environments where the public sector itself initiates and leads, rather than being pulled by market innovation.

A well-resourced public sector (higher PA expenditure) correlates strongly with AI initiatives, but we find no significant independent effect on blockchain initiatives. This suggests that simply injecting funding into public administration yields more AI projects (perhaps because AI solutions can be purchased or implemented if funds are available), whereas blockchain projects require more than just budget – they may need specific strategic intent or alignment with institutional reform goals. In practical terms, governments don't do blockchain projects just because they have money; they do them when there is a clear institutional rationale (e.g., creating a national digital ledger for certain services).

The cluster analysis and regression both indicate that blockchain projects are more often undertaken by central governments, while AI projects are relatively more common at the local government level. This was implicit in the cluster descriptions and is consistent with the idea that blockchain is being used for foundational state functions (often the purview of central agencies like interior ministries, land registries, national ID systems), whereas AI is being trialed to improve service delivery in various local contexts (city transport systems, regional healthcare analytics, municipal chatbots, etc.). This difference in institutional locus is a qualitative aspect that accompanies the quantitative findings.

At moderate levels of overall innovation, AI and blockchain can be complementary, an environment conducive to one tends to attempt the other as well. But in highly innovative environments, there appear to be trade-offs or specialization effects, likely due to resource allocation decisions. It is observed that when patent levels are very high, the positive association between AI and blockchain adoption turns negative, hinting that very advanced countries might channel efforts into whichever technology best fits their strategy, potentially to the exclusion of the other. These interaction effects reinforce that the institutional context and innovation strategy matter: they mediate how multiple technologies diffuse together.

Overall, the evidence strongly supports the notion that blockchain adoption in the public sector follows a distinct logic from AI adoption. In shorthand, AI behaves like a typical GPT, thriving on general innovation inputs and offering incremental improvements across many small applications, whereas blockchain behaves more like an institutional innovation, emerging where certain structural conditions and needs align (tech maturity on one hand, and possibly the absence of alternative solutions or a top-down push on the other).

2.5 Discussion

The analysis underscores that public-sector innovation remains highly path-dependent and institutionally embedded. Although blockchain is often presented as a General-Purpose Technology (GPT) with potential applicability across multiple domains, its empirical behaviour in government differs markedly from that of AI. AI adoption aligns with patterns typically associated with mature, data-intensive technologies: it tends to scale incrementally across units of government, responds positively to resource availability, and integrates into existing administrative routines without demanding significant institutional restructuring. Regression results confirm this logic: countries with higher levels of private R&D investment, stronger administrative capacity, and more developed innovation ecosystems tend to exhibit higher AI adoption.

In contrast, blockchain adoption in government displays a pattern that is both more selective and more institutionally oriented. The econometric models reveal that blockchain uptake is not driven primarily by the same innovation inputs that explain AI diffusion. Instead, blockchain adoption correlates more strongly with institutional conditions, such as governance quality, regulatory clarity, and public-administration centralization. These patterns suggest that the technology's value proposition in government lies less in computational performance and more in its ability to formalize, secure, or redesign institutional processes.

This divergence invites a broader theoretical reflection. The results suggest that blockchain may be moving along a developmental direction that departs from the trajectory expected of a conventional GPT. Rather than diffusing continuously as new data or computational capabilities become available, blockchain appears to be adopted when governments face specific institutional coordination problems that cannot be easily addressed with existing tools. In this sense, one could interpret the findings as pointing toward the emergence of a distinct problem-framing around blockchain in the public sector, one in which the technology is assessed not for its raw performance, but for its potential to reshape rules, interactions, and accountability structures.

This interpretation does not claim that blockchain has already established a new paradigm in public-sector technology. However, it does suggest that governments may be beginning to treat blockchain less as a generic digital tool and more as a mechanism capable of supporting institutional redesign. Such a shift, although still tentative, would help explain why blockchain adoption does not respond to the same incentives as AI and why it tends to appear in domains - such as identity, registries, and procurement - where institutional arrangements are central rather than peripheral.

Across all domains, public-sector blockchain adoption remains limited by the interlinked structural, organizational, and contextual barriers documented in the literature. As (Murano et al., 2025) show, obstacles cluster into four categories: organizational resistance and limited skills; interoperability and standards; innovation-specific complexity; and regulatory or contextual uncertainty. These challenges highlight that blockchain implementation requires more than technical upgrades. Where blockchain is pursued, it often acts as a catalyst for

institutional change, prompting governments to reconsider processes, roles, and governance arrangements.

In this sense, the findings reinforce the idea that digital transformation in government is not solely a matter of adopting better tools, but also of adapting institutional structures. Blockchain, perhaps more than AI, makes this interplay visible: the type of public value it promises cannot be fully realized unless institutions are willing to evolve in parallel.

2.6 Policy implications

These findings have direct implications for public-sector digital policy. First, governments should avoid treating different technologies as interchangeable and should develop strategies tailored to their distinct logics of adoption and impact. For AI - modular, data-driven, and highly scalable technology - policy can focus on strengthening complementary assets. This includes improving data governance, investing in computational infrastructure, upskilling public-sector workers, and fostering partnerships with private firms. Local experimentation is particularly effective for AI, given its capacity to deliver incremental improvements within established administrative routines.

Blockchain requires a different approach. Given the results, blockchain should be treated less as an off-the-shelf digital tool and more as a potential enabler of institutional redesign in specific domains. Policymakers aiming to leverage blockchain should therefore consider measures that go beyond technical procurement, such as updating legal frameworks, clarifying the regulatory status of digitally signed and time-stamped records, and promoting inter-agency collaboration.

The econometric findings also imply that blockchain adoption is more successful when it is aligned with clearly articulated institutional needs - such as enhancing accountability, strengthening auditability, or improving multi-party coordination - rather than when it is introduced generically as an innovation initiative. For this reason, governments should identify high-value domains where existing institutional arrangements impose persistent frictions and evaluate whether blockchain's properties meaningfully address those frictions.

Finally, policymakers should adopt evaluation frameworks that reflect each technology's nature. AI projects can be assessed through efficiency metrics, accuracy improvements, or user satisfaction. Blockchain initiatives, instead, should be evaluated through governance-oriented metrics - transparency gains, reduction in procedural vulnerabilities, or improvements in record integrity - since these are the areas where the technology demonstrates its distinctive contribution.

2.7 Conclusion

The empirical evidence of this study reveals a clear divergence in the underlying drivers, patterns, and institutional conditions associated with the diffusion of the two technologies. AI behaves as a consolidated GPT in government: its adoption correlates strongly with traditional indicators of innovation capacity, such as private R&D investment, robust administrative resources, and mature technological ecosystems. These results are consistent with AI's

modular and data-intensive nature, which enables the technology to integrate smoothly into existing bureaucratic routines and to deliver incremental performance gains without requiring substantial institutional change. In the language of innovation theory, AI diffusion follows a cumulative trajectory rooted in a stable computational paradigm, where improvements stem from refinements to established heuristics rather than from disruptions to institutional architectures.

Blockchain, by contrast, exhibits a diffusion pattern that is both more selective and more institutionally shaped. Its adoption is not strongly associated with conventional innovation inputs and does not behave like a tool that scales proportionally with technological maturity or resource availability. Instead, blockchain uptake appears closely linked to institutional variables such as governance quality, regulatory clarity, and the presence of centralised administrative structures. Governments deploy blockchain in domains - such as identity management, public registries, procurement, and multi-agency coordination - where institutional arrangements are foundational rather than peripheral. This empirical pattern suggests that blockchain is not perceived as a generic digital solution but as a technology with implications for how public-sector rules, procedures, and accountability mechanisms are structured. In these contexts, blockchain is adopted not because it provides superior computational performance, but because it offers a way of addressing institutional coordination problems that existing tools cannot easily resolve.

This contrast resonates strongly with the theoretical framework introduced at the beginning of the paper. Drawing on (Dosi, 1982) distinction between technological paradigms and trajectories, AI appears to follow a conventional trajectory within a consolidated paradigm, one where technological progress accumulates incrementally, guided by established cognitive heuristics. Blockchain, instead, seems to occupy a more ambiguous position: while not yet constituting a new paradigm, its public-sector adoption increasingly reflects a redefinition of relevant problem spaces and heuristics. Governments are not merely extending the existing computational paradigm when adopting blockchain: they may be engaging with the technology in ways that are consistent with a partial redefinition of relevant problem spaces toward institutional design and rule configuration. Given the cross-sectional nature of the evidence, this should be interpreted as suggestive of an emerging institutional framing in public-sector contexts rather than as confirmation of a paradigmatic discontinuity.

This evolving dynamic does not imply that blockchain has already produced a paradigmatic rupture, but it does point to a distinct problem-framing in which blockchain is evaluated for its capacity to underpin institutional transformation rather than merely enhance computational efficiency. The econometric findings reinforce this interpretation: blockchain adoption increases where institutional incentives - such as the need for trustworthy records, transparent procedures, or tamper-resistant auditability - are especially salient and not necessarily where technological or financial resources are abundant. Moreover, blockchain initiatives often emerge in tandem with administrative or legal reforms, revealing a pattern in which technological uptake and institutional adjustment are mutually reinforcing. In contrast, AI adoption tends to involve minimal structural redesign and fits squarely within the logic of an efficiency-enhancing technology.

A central limitation of this chapter is the cross-sectional nature of the dataset. The analysis captures differences across countries at a given point in time, but it cannot observe how blockchain adoption and institutional embedding evolve within countries. As a result, the findings cannot establish whether the incorporation of blockchain into public administration produces gradual changes in governance over time, nor can they capture path-dependent learning trajectories, delayed effects, or sequencing dynamics. The results should therefore be interpreted as evidence of differential adoption correlates and problem-framings, rather than as evidence of dynamic institutional transformation. Longitudinal data (panel or time-series designs) would be required to directly assess governance change over time.

Taken together, these results suggest that blockchain's value in the public sector is closely tied to its ability to support new forms of institutional coordination, rather than its performance as a purely technical artefact. The comparison with AI makes this distinction particularly visible: while AI strengthens existing administrative capacities, blockchain encourages governments to rethink foundational processes and governance arrangements. This opens an important avenue for future research. The evidence presented here suggests that blockchain may be developing along a trajectory that departs from the prevailing technological paradigm, moving instead toward an applied direction in which institutional considerations - not technological performance alone - play a defining role. Clarifying whether this emergent direction stabilises into a coherent paradigm or remains a context-specific pattern represents a promising line of inquiry at the intersection of innovation studies and public governance.

From a policy perspective, the findings underscore the need for differentiated digital strategies. AI can generally be integrated through investments in capability, data governance, and interoperability within existing frameworks, whereas blockchain demands strategic alignment with specific institutional objectives and often requires legal and procedural adaptation. Policymakers treating the two technologies as if they shared the same logic of diffusion risk misallocating resources or failing to anticipate the institutional adjustments required for successful blockchain implementation.

In conclusion, the comparative evidence demonstrates that while AI operates as a mature GPT that reinforces established administrative capacities, blockchain follows an emergent trajectory whose driving forces are institutional rather than purely technological. This pattern is consistent with an early-stage reorientation of the technological problem-space, echoing insight that shifts in heuristics and problem definitions often precede broader paradigmatic change. Recognising this evolving dynamic - and exploring whether it consolidates into a distinct institutional trajectory - represents a significant opportunity for future research on digital innovation, institutional economics, and public-sector transformation.

CHAPTER 3

The evolution of organizations and blockchain: a multilevel framework

The comparative analysis in Chapter 2 offers macro-level evidence that institutional conditions shape the diffusion of blockchain and AI. These findings set the foundation for the next step in the thesis: a shift from broad patterns of national adoption to the organizational consequences of blockchain technology.

Chapter 3 ² develops a new theoretical framework that examines blockchain's impact at the micro and meso levels of organizational design. At the core of this framework is the "V-Form" organization, an original model for a blockchain-enabled structure. While the previous analysis highlighted cross-country differences in adoption, the focus here is on how independent actors can coordinate, generate trust, and govern shared activities through blockchain protocols rather than conventional hierarchies or contractual systems.

The V-Form concept contributes a novel paradigm to organization theory, envisioning governance embedded in transparent code and decisions distributed across participants. It explicitly links individual incentives to institutional structure, showing how the behaviours observed empirically in Chapter 2 can be aligned through blockchain mechanisms to produce a coherent, trust-generating organizational form.

Overall, the transition from Chapter 2 to Chapter 3 marks a movement from empirical observation to conceptual synthesis. Insights about institutional adoption inform the design of a new organizational model tailored to the blockchain era.

3.1 Introduction

Economic organizations can be understood as complex adaptive systems whose structures and behaviours emerge from multi-level interactions. Traditional analyses often focused on either macro-level outcomes or micro-level behaviour in isolation, but some theoretical perspectives emphasize a micro–meso–macro architecture to capture the full complexity of economic evolution. In this view, an economy is seen as a rule-system (meso) carried by individual agents (micro), producing aggregate structures (macro) (Dopfer et al., 2005).

Adopting this lens, the evolution of organizational forms and the impact of blockchain technology is analysed. It bridges meso-level models with micro-level transaction dynamics to examine how trust and coordination mechanisms propagate from individual behaviour to systemic change.

² An earlier version of the analytical framework developed in this chapter was presented as a conference paper: Murano, A. (2025), *Blockchain, Trust and Organisations: Implications for Economic Coordination*, Proceedings of the 51st EBES Conference (Rome, 11–13 April 2025), ISBN: 978-625-95653-1-6. The present chapter substantially expands the theoretical model and situates it within the broader institutional perspective of the dissertation.

The study has three goals: (i) to trace the progression from the U-form to the blockchain-enabled V-form; (ii) to compare their cost structures under varying trust conditions; (iii.) to examine how individual micro-level decisions influence the evolution of trust mechanisms, leading to the emergence of new coordination dynamics at the meso-organizational level. By moving from meso (organizational form) to micro (agent transactions), the analysis justifies how emerging technologies necessitate more granular analysis: trust is fundamentally a micro-level phenomenon in transactions, yet it defines the viability of entire organizational forms at the meso level.

Blockchain is framed as an institutional technology (Davidson et al., 2018) that reconfigures economic organization. Organizational forms are treated as rule systems whose viability depends on agent incentives. The framework demonstrates how decentralized governance protocols reduce coordination and trust costs. Linking micro-level behaviour to meso-level structures provides a dynamic view of organizational evolution under technological change.

While traditional firms internalized trust through hierarchy and culture, blockchain allows trust to emerge externally through protocol design (Berg et al., 2020). This shift motivates a micro-level analysis of transactions within complex rule-based systems, focusing on how blockchain reshapes the cost and trust calculus at the transactional level. In this chapter an interdisciplinary approach integrating economic and computer science perspectives is adopted. It focuses on permissioned, non-cryptocurrency applications of blockchain, treating nodes as economic agents whose behaviour responds to incentive constraints. Effective design must ensure incentive compatibility to align individual and system goals. The chapter is structured as follows. Section 3.2 traces the historical evolution of organizational forms. Section 3.3 introduces the micro–meso analytical framework. Section 3.4 reframes blockchain as an institutional technology. Section 3.5 presents theoretical conclusions and Section 3.6 explores research and policy implications.

3.2 Evolution of organizational forms

Organizational forms have co-evolved with economic, technological, and institutional changes. Each form addressing limitations of the prior and introducing new trade-offs. The historical progression is outlined through four ideal types – U-Form, M-Form, VO, and V-Form – and the factors driving each transition.

3.2.1 U-Form

The U-Form organization, dominant in early industrial capitalism, featured centralized hierarchies managing specialized departments (O. E. Williamson, 1983).

It emerged alongside the shift from artisanal to factory production, driven by mechanization, labour concentration, and scale economies (Chandler, 1977). Coordination relied on hierarchical authority, with decision-making concentrated among owners and supervisors (Marglin, 1974). Initially based on practical experience, not scientific structuring (Landes, 1969), labour organization evolved with growing scale and demand, prompting the adoption of scientific management (Pollard, 1968).

Taylor's time-and-motion studies standardized tasks, reduced discretion, and introduced a management layer for monitoring (Nelson & Winter, 1985; Taylor, F. W., 1911). This paradigm shift formalized the separation between planning and execution, institutionalizing a new management layer dedicated to monitoring compliance (Edwards, 1982). This boosted efficiency but also led to deskilling and alienation (Braverman, 1998).

The U-Form thrived in settings requiring uniformity and scale, enabling functional specialization and rule-based coordination. Yet, its centralized structure became a liability as complexity grew. It struggled with diversified products and dispersed operations, causing decision bottlenecks and reducing adaptability (O. E. Williamson, 1983).

Though essential to industrial development, the U-Form's rigidity and inefficiencies eventually paved the way for more flexible structures like the M-Form, better suited to dynamic environments.

3.2.2 M-Form

The M-Form emerged mid-20th century to overcome the U-Form's limitations amid growth, diversification, and geographic expansion (Chandler, 1977; O. E. Williamson, 1975). Centralized decision-making had become inefficient, leading to coordination bottlenecks and information overload.

By decentralizing operations into semi-autonomous units - organized by product, region, or customer - the M-Form enabled localized decision-making while corporate HQ focused on strategy and capital allocation (Hill & Hoskisson, 1987). This structure improved accountability, reduced opportunism, and enhanced coordination (O. E. Williamson, 1963) allowing firms to balance scale with adaptability.

Its key strength lay in enabling parallel innovation and responsiveness across divisions. However, it also brought higher administrative costs and functional redundancies, as shared resources became fragmented and internal competition could arise.

Pioneered by firms like General Motors and DuPont, the M-Form influenced global organizational design (Fligstein, 2000; Kogut & Parkinson, 1998). Many firms later adopted hybrids to reconcile functional efficiency with divisional flexibility.

In a similar perspective, Toyotism introduced JIT, jidoka, and kaizen, focusing on flexibility, quality, and worker-driven problem-solving (Ohno, 1988; Rüttimann & Stöckli, 2016). It responded effectively to volatile demand and customization, evolving into the lean production paradigm (Womack et al., 2007).

Overall, the M-Form marked a pivotal step in organizational evolution, enabling decentralized governance and operational flexibility, setting the stage for further digitally enabled forms.

3.2.3 Virtual Organization

The shift from U-Form to M-Form addressed early coordination issues, but by the late 20th century, globalization, customization, and digitalization exposed new limits. These changes spurred organizational experimentation beyond firm boundaries.

One such model was the Virtual Organization (VO): a network of independent firms collaborating without centralized ownership or hierarchy (Davidow & Malone, 1992; Saabeel et al., 2002). Enabled by ICT, VOs aimed for high flexibility, contracting out non-core functions and leveraging global expertise (Franke, 2001; Khalil & Wang, 2002). Theoretically, reduced coordination costs would allow market mechanisms to replace hierarchy.

However, VOs struggled in practice. Their reliance on trust and shared norms clashed with the temporary, dispersed, and cross-cultural nature of their networks (Goldman et al., 1995; Riemer & Klein, 2008). Legal and governance systems proved ill-suited to support their fluidity, leaving VOs exposed to opportunism, weak monitoring, and contractual breakdowns (Chi et al., 2003; Tuma, 1998). Without stable internal governance, they lacked mechanisms to enforce norms and manage risk (Bartlett & Ghoshal, 1993; O. E. Williamson, 1996).

By the early 2000s, enthusiasm faded. Although globalization and digital technologies had clearly transformed the boundaries and operations of the firm (Bleecker, 1994; Venkatraman & Henderson, 1998), VO model gave way to more structured ecosystems and platform organizations, typically anchored by a central coordinator. These entities better managed trust through clearer governance and institutional support.

Despite its shortcomings, VO highlighted the importance of horizontal, cross-boundary collaboration and value co-creation. Yet it also revealed a key problem: how to scale trust in decentralized systems. This unresolved challenge sets the stage for the V-Form, which leverages blockchain to embed trust directly into its infrastructure.

3.2.4 V-Form

VO introduced flexible, inter-firm collaboration but lacked scalable trust mechanisms. Blockchain and distributed ledger technologies (DLTs)³ address this by turning trust into a technological function, enabling a new model: the V-Form (Berg et al., 2018),

V-Form is a vertically non-integrated structure where coordination is achieved through blockchain rather than hierarchy or contracts. Smart contracts and consensus protocols replace traditional firm functions like quality control and enforcement. This shifts vertical integration onto decentralized infrastructure, transforming how value is coordinated.

Unlike earlier models that relied on trust and bilateral agreements, V-Form “industrialize” trust via immutable, verifiable ledgers (Berg et al., 2020). Automated rules reduce opportunism and enable market-like incentives within coordinated ecosystems.

A key feature is the use of shared, time-stamped data across actors in a supply chain - suppliers, auditors, logistics providers - who interact through the same verified information. In

³ Distributed ledger technologies (DLTs) refer to shared ledgers replicated across multiple nodes, where updates are validated through agreed procedures rather than a single central administrator. “Blockchain” is a prominent DLT family characterized by cryptographically linked blocks and consensus-based state updates.

blockchain consortia, for example, transactions trigger automated actions like payments or compliance checks, removing the need for centralized oversight (Abeyratne & Monfared, 2016). A key example of the V-form is the IBM-Maersk project, where multiple logistics firms use a shared blockchain for shipping data management (Allison, 2018). This enables cross-organizational coordination while preserving legal independence and data privacy.

Unlike the M-form, which coordinates through internal hierarchies (Chandler, 1966; O. E. Williamson, 1996), the V-form links autonomous entities via shared digital protocols. Coordination occurs through blockchain validation, not managerial commands. Smart contracts automate business logic, reducing agency costs and boosting responsiveness.

Yet, challenges persist. Standardization of data formats, identity, and permissions is essential but difficult (Riemer & Klein, 2008). Firms may hesitate to share sensitive information, fearing competitive risks. As a result, many V-form networks retain a lead orchestrator, creating a hybrid between decentralization and traditional oversight.

Legal uncertainty also limits adoption. Blockchain protocols often fall short of regulatory norms on liability, dispute resolution, and data privacy. Public blockchains offer openness and auditability but face latency and scalability issues; consortium models offer control but compromise decentralization.

Despite challenges, V-form redefines economic coordination. Following (North, 1990) and extending transaction cost economics (O. E. Williamson, 1996), it positions blockchain as an institutional layer that reshapes the boundaries between firms, markets, and networks.

Rather than relying on ownership and authority, V-form externalizes hierarchy through code and consensus. Trust and enforcement shift from internal structures to transparent, programmable infrastructure.

This model suits sectors demanding traceability, automation, and disintermediation, such as pharma, agribusiness, logistics, and finance. As scalability and interoperability advance, V-form organizations may increasingly supplement or replace traditional firms.

3.3 Methodology: Micro–Meso analytical framework

To rigorously compare these organizational forms, micro–meso–macro framework from evolutionary economics (Dopfer et al., 2005) is adopted. This framework was considered suitable because it explicitly accounts for how individual behaviours aggregate into collective structures, capturing the complex and emergent properties of organizational change. In this architecture, meso corresponds to rule populations, micro to individual rule-carriers, and macro to the aggregate outcomes of rule dynamics. Each organizational form is treated as a generic rule or institutional template that can be adopted by many actors, for example, the set of coordination practices defining a U-form is a rule, and all firms using a U-form constitute its population of carriers.

This methodology combines a meso-level comparative analysis of institutional cost regimes with a micro-level adaptive model of agent decision-making. This reflects a complexity-focused paradigm in institutional analysis, moving beyond static equilibrium to study process

and evolution (Frolov, 2021). In this way, a more theoretically coherent and operationally detailed understanding is pursued of how emerging technologies – specifically blockchain - can trigger shifts in the dominant mode of economic organization.

Notably, the micro-level aspect of our framework particularly benefits from an interdisciplinary lens, drawing an explicit parallel between algorithmic consensus rules and economic governance mechanisms. This analogy ensures that the model captures the self-interested behaviour of validators through both technical and economic perspectives, reflecting how consensus design incorporates incentive compatibility (Murano et al., 2024).

The analytical framework builds on and extends the perspective proposed by (Dopfer et al., 2005), wherein economic coordination is analysed through the lens of rule systems and their carriers. While that ontological structure is adopted, the contribution here consists in operationalizing it in a formal, cost-driven model of organizational choice. Specifically, organizational archetypes are modelled as evolving coordination rules whose adoption depends on micro-level incentives and meso-level cost structures. This approach enables a dynamic analysis of institutional innovation under technological change.

Thus, to clarify the analytical units and their relationships, the following definitions are provided:

Rule: A shared instruction or practice that agents follow. In our context, an organizational archetype is a rule that can spread or be replaced. The meso-level focuses on these rules and their population dynamics. Here, each organizational form can be seen as a rule encoding a particular coordination mechanism.

Rule-Carriers: The agents or organizations that adopt and implement a rule. At the micro level, these carriers include individual decision-makers, such as entrepreneurs, managers, or autonomous smart agents within a Decentralized Autonomous Organization (DAO)⁴ (Wang et al., 2019)). These actors decide how to organize transactions, effectively selecting and enacting specific organizational rules. For example, a firm's managers might implement an M-form structure, while a group of decentralized agents may coordinate through a V-form consortium. The interactions and decisions of these rule-carriers generate feedback effects that influence which organizational forms gain prominence over time.

Rule-Population: The set of all carriers following a given rule, which constitutes the meso unit of analysis. For example, all firms globally that use a multidivisional structure form the population associated with the M-form rule. The size and success of a rule-population can change over time as new firms adopt a form or existing firms abandon it. The model developed will represent how these populations evolve when a new rule competes with established ones.

⁴ A DAO is an organizational arrangement in which defined governance procedures and decision rights are implemented through smart contracts and (often) on-chain voting mechanisms; in practice, the degree of decentralization varies with governance design and control of upgrades/treasury.

Coordination Mechanism: The institutional logic by which transactions are coordinated under a given rule. This is essentially the content of the rule. The coordination mechanism determines the distribution of information and the way incentives are aligned among participants (Qian et al., 2003).

Using micro–meso approach, organizational forms can be formally compared based on their cost structures and transitions can be analysed as an evolutionary process. The methodological rationale is twofold. First, by expressing each form in terms of cost functions, a common quantitative measure is obtained to evaluate efficiency under various conditions (e.g. how total costs scale with size or trust requirements). This builds on classic transaction cost economics: firms exist when they can perform transactions internally at lower cost than the market (Coase, 1937). The cost-based models presented here extend that logic to include trust mechanisms explicitly, which is essential for distinguishing VO and V-form. Second, by embedding these cost functions into an evolutionary game model, we capture how agents might shift between organizational rules over time rather than assuming static choice. This dynamic approach recognizes that organizational forms compete in a population: if one form yields consistently lower costs (higher payoffs) in a given environment, agents will tend to adopt it, increasing its prevalence. Such modelling allows the examination of transitional trajectories, for example, how rapidly a new V-form might overtake traditional firms, or whether multiple forms can coexist in equilibrium.

3.3.1 Meso-organizational model: cost structures of different forms

To compare organizational archetypes through a unified and rigorous analytical lens, this section develops a meso-level model that integrates both a formal mathematical structure and organizational interpretation. The purpose is twofold: first, to formalize how coordination and trust costs jointly determine the efficiency of different organizational forms; second, to interpret how these formal mechanisms represent the underlying economic and institutional logic of coordination.

At the meso level, organizations are conceptualized as rule systems, institutionalized templates that coordinate economic activity through specific mechanisms of control, information sharing, and trust enforcement. Each archetype (U-form, M-form, VO, and V-form) embodies a distinctive balance between coordination costs, which reflect the resources needed to align actions across units, and trust mechanism costs, which represent the resources required to ensure reliable behaviour and prevent opportunism. The model thus translates organizational theory into a cost-based formalization, while the organizational interpretation reintroduces its economic and institutional meaning.

Formally, for any given organizational form, the total cost of managing a given number of transactions can be expressed as:

$$\text{Total Cost}^{(form)} = C_{\text{coord}}^{(form)} + C_{\text{trust}}^{(form)} \quad (2)$$

where $C_{\text{coord}}^{(form)}$ represents the cost of coordinating interdependent activities, and $C_{\text{trust}}^{(form)}$ the cost of maintaining or enforcing trust among agents. Economically, these two dimensions correspond to the dual functions of the firm as theorized by (Coase, 1937; O. E. Williamson, 1996): internal coordination substitutes for market transactions when it lowers total costs, but it simultaneously introduces internal control and monitoring overheads.

3.3.2 Organizational cost components

The coordination cost encompasses managerial, communicative, and procedural efforts necessary to integrate decisions across organizational units. The trust mechanism cost, by contrast, depends on the institutional or technological infrastructure required to secure transactions and limit opportunistic behaviour.

Trust is treated as an exogenous variable ⁵ T , representing the background level of confidence existing in the environment. The mechanism M implemented by the organization modifies this trust level, and its cost $M(T)$ varies inversely with T : when trust is scarce, the mechanism becomes costlier. Thus, the general model is expressed as:

$$\text{Total Cost} = C + M(T) \quad (3)$$

where higher T (trust) reduces $M(T)$, while lower T requires either expensive monitoring or sophisticated institutional mechanisms (such as blockchain). From an economic-organizational perspective, this formulation captures a fundamental trade-off: hierarchical systems internalize trust through authority (low $C_{\text{trust}}^{(form)}$, high $C_{\text{coord}}^{(form)}$), whereas market- or network-based systems externalize coordination (low $C_{\text{coord}}^{(form)}$) but face higher trust costs due to weaker enforcement. Blockchain-enabled forms, as shown later, modify this balance by embedding trust within protocol-level coordination.

3.3.3 Formal representation of organizational archetypes

The general structure of the model applies to each organizational archetype, each defined by its coordination unit and corresponding trust mechanism.

U-Form

⁵ For analytical tractability, Sections 3.3.2–3.3.3 treat T as an environmental parameter affecting the marginal cost of monitoring/enforcement. Section 3.3.6 subsequently micro-founds (endogenizes) trust by linking it to validator behavior, incentive alignment, and protocol/governance design.

The U-Form represents a centralized hierarchical structure where decision-making and control are vertically integrated. Formally:

$$C = \alpha N \quad (4)$$

where N denotes the number of workers or operational units and α the per-unit coordination cost.

Since control is direct, the trust mechanism is based on monitoring, with cost:

$$M(T) = \beta N \quad (5)$$

where β is the per-unit monitoring cost.

Hence, total cost:

$$\text{Total Cost}_{\text{U-Form}} = C + M(T) = \alpha N + \beta N = (\alpha + \beta)N \quad (6)$$

It is possible to note that this structure minimizes relational uncertainty: trust is substituted by authority and supervision. The hierarchy itself enforces compliance, so opportunism is limited internally. Yet, as scale increases, coordination costs rise disproportionately, leading to inefficiency in complex environments. The model thus formalizes the historical trajectory from efficient industrial bureaucracies to increasingly rigid structures under informational overload.

M-Form

The M-Form introduces a semi-decentralized logic, dividing the firm into autonomous divisions. Formally:

$$C = \alpha D \quad (7)$$

where D is the number of divisions. Trust is ensured by incentive alignment - for example, through divisional profit/efficiency targets, performance-based compensation, internal auditing, and control systems that link managerial payoffs to organizational objectives - whose cost decreases with the level of trust T :

$$M(T) = \frac{\lambda}{T} \quad (8)$$

where λ represents the risk of managerial opportunism or misalignment.

Therefore:

$$\text{Total Cost}_{\text{M-Form}} = \alpha D + \frac{\lambda}{T} \quad (9)$$

Economically, this model captures the logic of corporate decentralization: divisions operate semi-independently, reducing coordination overload at the top, but requiring incentive schemes to align interests. When trust within divisions is high, monitoring needs fall, making M-form efficient; when trust declines, incentive systems must be strengthened, raising costs. The equation formalizes this dynamic tension between autonomy and control.

Virtual Organization (VO)

The VO extends coordination beyond firm boundaries, forming networks of autonomous entities.

Formally:

$$C = \alpha V \quad (10)$$

$$M(T) = (C_{\text{Cons}} + C_{\text{Ver}})V \quad (11)$$

where V represents the number of partner units, C_{Cons} the cost of maintaining cooperation and information consistency, and C_{Ver} the cost of verification and legal compliance. Thus:

$$\begin{aligned} \text{Total Cost}_{\text{VO}} &= \alpha V + (C_{\text{Cons}} + C_{\text{Ver}})V = \\ &V [\alpha + (C_{\text{Cons}} + C_{\text{Ver}})] \end{aligned} \quad (12)$$

Conceptually, the VO relies on external enforcement - contracts, audits, and certification - to sustain collaboration. While coordination across specialized units remains flexible, trust costs increase with network complexity and environmental uncertainty. The model illustrates why purely virtual organizations, despite theoretical efficiency, have struggled in practice: they remain vulnerable to opportunism when institutional trust is weak.

V-Form (Blockchain-enabled VO)

The V-Form introduces blockchain as an institutional technology that embeds coordination and trust enforcement into the protocol layer. Formally:

$$C = \alpha V + C_{setup}$$

$$M(T) = (C_{cons}^{tech} + C_{ver}^{tech})V^{\beta} \quad (13)$$

$$\text{Total Cost}_{V\text{-Form}} = \alpha V + C_{setup} + (C_{cons}^{tech} + C_{ver}^{tech})V^{\beta} \quad (14)$$

Here, C_{setup} represents fixed technological and integration costs (e.g., protocol engineering, systems integration with legacy infrastructures, cybersecurity hardening, and the “translation” of governance/verification requirements into auditable code and procedures). The term $(C_{cons}^{tech} + C_{ver}^{tech})$ captures recurring technological costs of maintaining consensus and verification, while the exponent β ($0 < \beta \leq 1$) captures how these costs scale with network size: when infrastructure, standards, and governance routines mature, marginal verification/coordination burdens can scale less than proportionally ($\beta < 1$) due to automation and reusability.

This formalization makes explicit what distinguishes the V-Form from the VO: whereas the VO’s trust mechanism costs are dominated by external legal/administrative enforcement (contracts, audits, certification), the V-Form substitutes a share of those costs with technological set-up and protocol-operation costs, and its efficiency hinges on whether these technological costs can be governed and amortized across participants.

In this perspective, blockchain “industrializes trust” - in the perspective of (Berg et al., 2017) - by making verification endogenous to the system. Consensus protocols and cryptographic validation replace third-party enforcement, enabling autonomous entities to cooperate reliably without hierarchical oversight. In low-trust environments, this transformation is particularly advantageous: while U- and M-forms internalize trust through costly hierarchy, and VOs suffer from contractual fragility, the V-Form externalizes trust to a shared technological infrastructure that remains transparent, auditable, and tamper-resistant.

Table 5 emphasizes the key differences among the archetypes:

Organizational Archetype	Organizational Unit	Coordination Cost (C)	Trust Mechanism Cost (M(T))	Trust Mechanism (M)	Focus
U-Form	Workers	$C = \alpha N$	$M(T) = \beta N$	Direct supervision and hierarchical control	Rigid supervision, centralized structure
M-Form	Divisions	$C = \alpha D$	$M(T) = \frac{\lambda}{T}$	Incentive structures to align divisions	Strategic autonomy.

Organizational Archetype	Organizational Unit	Coordination Cost (C)	Trust Mechanism Cost ($M(T)$)	Trust Mechanism (M)	Focus
					Trust ensured via incentives
VO (Virtual Organization)	Nodes	$C = \alpha V$	$M(T) = (C_{Cons} + C_{Ver})V$	External enforcement via legal/institutional intermediaries (contracts, audits, certification)	Decentralized cooperation relying on third-party trust
V-Form (Blockchain- enabled VO)	Nodes	$C = \alpha V$	$M(T) = (C_{cons}^{tech} + C_{ver}^{tech})V^\beta$	Endogenous enforcement via protocol (blockchain consensus, smart contracts)	Full decentralization. Trust embedded and automated through code

Table 5 - Comparison of the different archetypes within the model

3.3.4 Interpretation and results

The integrated model shows that the total cost of any organizational form depends on the interplay between coordination effort C , trust mechanism cost $M(T)$, and the nature of the trust mechanism M itself. Each form represents a distinct institutional configuration balancing hierarchy, autonomy, and technological mediation.

In hierarchical forms (U- and M-Form), trust enforcement relies on authority and internalized control, leading to scalability limits due to coordination overhead. In networked forms (VO and V-Form), coordination is distributed, but trust must be externally guaranteed—unless it is embedded technologically, as in the blockchain-based V-Form.

The model reveals that blockchain fundamentally transforms the cost structure of trust. In traditional VO settings, verification requires external mechanisms - contracts, audits, and legal enforcement - whose cost grows linearly with network size. In the V-Form, these mechanisms are replaced by computational trust: cryptographic validation and decentralized consensus, which scale efficiently and distribute verification costs across the network.

In the formal representation introduced above, this transformation is captured by the presence of a fixed technological cost C_{setup} and by recurring technological costs of consensus and verification ($C_{cons}^{tech} + C_{ver}^{tech}$), which scale with network size according to the exponent β (with $0 < \beta \leq 1$). While traditional monitoring and enforcement costs tend to increase proportionally with organizational scope, blockchain-based coordination allows these costs to grow more slowly when technological infrastructure and governance routines mature (i.e., when $\beta < 1$). Formally, the V-Form achieves a lower per-unit coordination cost than traditional hierarchical or contractual arrangements when the technological cost component $M(T) = (C_{cons}^{tech} + C_{ver}^{tech})V^\beta$ grows more slowly than the monitoring and enforcement costs associated with hierarchical oversight. Economically, this means that blockchain enables organizations to expand horizontally - adding autonomous partners or nodes - while limiting the increase in coordination and verification costs relative to organizational scale.

Thus, while the U-Form and M-Form achieve control through vertical integration, and the VO depends on external institutions, the V-Form replaces both hierarchy and third parties with protocol-based governance. Trust becomes an engineered property of the infrastructure rather than a social or legal assumption, enabling scalable cooperation among independent actors.

In conclusion, the meso-organizational model formally demonstrates how blockchain reconfigures the economics of coordination and trust. By externalizing enforcement to code, it reduces the transaction costs that once justified firm boundaries. This translates into a new organizational paradigm where trust is no longer a scarce relational asset, but a programmable and collectively produced resource, redefining the institutional logic of cooperation itself.

3.3.5 Micro-individual model: from validator behaviour to emergent organizational trust

The meso-level model previously introduced characterizes how decentralized, blockchain-based governance can reduce enforcement costs and improve organizational efficiency by institutionalizing trust through technology. However, this framework treats trust as an exogenous parameter, acting as a given condition rather than a dynamic outcome.

In this section, the analysis moves to the micro-foundations of trust by explicitly modelling how individual behaviours within decentralized architectures, namely those of validators, give rise to collective trust dynamics. This allows to open the organizational black box and explain how trust emerges rather than simply assuming its presence.

In this perspective, meso-level describes what happens (e.g., lower costs, greater coordination) and micro-level explains how it happens, through agent-level decisions governed by smart contracts.

This micro-level model is inherently interdisciplinary in nature: it reconceptualizes the blockchain consensus process as an institutional mechanism for aligning self-interested agents. In other words, the consensus algorithm functions as a built-in incentive scheme that

coordinates validator behaviour, analogous to how contracts or governance policies align employees' actions with a firm's objectives.

3.3.6 Endogenizing trust: micro-level dynamics in validator behaviour

The idea is to model an organization populated by N validators, agents responsible for approving or rejecting discrete events (e.g., ledger entries, financial records, supply chain updates). Each validator i selects an action $a_i \in \{0,1\}$, where:

$a_i = 1$ denotes approval.

$a_i = 0$ denotes rejection of a given event.

Building on a framework derived from computer science, particularly consensus protocols such as PBFT⁶ embedded in blockchain systems (Murano et al., 2024), a collective outcome is considered validated when the proportion of approvals $A = \sum a_i / N$ exceeds a qualified majority threshold θ , typically $\theta = 2/3$.

Validators are differentiated by behavioural types:

Honest: act according to verifiable criteria and collective integrity.

Faulty: act to maximize private payoff, even at the expense of system integrity.

Each agent maximizes a dual-component utility function:

$$U_i = u(a_i, v) + m(a_i, R) \quad (15)$$

Where:

$u(a_i, v)$: intrinsic utility tied to alignment with block validity v ;

$m(a_i, R)$: extrinsic monetary incentive as defined by the reward scheme R .

We compare two stylized reward architectures:

Scheme A: Approval-Based Incentives. Validators are rewarded if they vote yes and the block is approved, regardless of the block's true validity. This scheme promotes throughput, but vulnerable to superficial validation.

Scheme B: Truth-Aligned Incentives. Rewards are issued only when a validator's vote aligns with the true status of the block. This scheme encourages accuracy, though may reduce speed.

⁶ PBFT denotes a class of Byzantine-fault-tolerant consensus protocols typically used in permissioned settings, where agreement is reached via message exchange and the protocol tolerates a bounded number of faulty/malicious nodes under stated assumptions.

Following the framework proposed in (Murano et al., 2024) is possible to demonstrate that the remuneration scheme A is not incentive compatible for honest nodes, who will prefer to accept also false blocks, also when considering expected payoffs. The false block rejection will depend on the validator's preferences and on the blockchain dimension. Conversely, the second scheme (B) is incentive compatible for honest nodes, who have a dominant strategy in accepting valid blocks and rejecting false blocks. Faulty nodes will always agree on false block acceptance, whereas the rejection of valid blocks is conditioned.

In blockchain-enabled V-Form architectures, such incentive schemes could be embedded in the protocol via smart contracts, which also monitor validator reputation over time.

This feedback loop encourages honest behaviour not merely for immediate gain, but as a strategy to maintain long-term credibility and inclusion in the governance structure.

3.3.7 Aggregation mechanism: from behaviour to trust

Individual-level decisions influence the evolution of systemic trust, captured by the following recursive dynamic:

$$T_{t+1} = T_t + \gamma(H_t - F_t) \quad (16)$$

Where:

T_t : level of institutional trust at time t ;

H_t, F_t : shares of honest and opportunistic validators at time t ;

γ : sensitivity parameter of the system to net honest behavior.

Trust accumulates when the honest share exceeds the opportunistic one, it deteriorates otherwise.

Essentially, as T increases, enforcement costs - formal controls, audits, and manual verifications - decline according to the meso-level function:

$$M(T) = \frac{\lambda}{T + \varepsilon} \quad (17)$$

This feedback loop operationalizes the micro-meso linkage, establishing a bidirectional relationship in which emergent trust dynamics at the micro level both shape and are shaped by meso-level rule selection and propagation.

3.3.8 Linking micro behaviour to meso outcomes

The combined model reveals a dynamic trajectory of trust formation and organizational transformation; wherein micro-level decisions and meso-level rule evolution are mutually reinforcing. The following table illustrates this bidirectional relationship: agent-level behaviour

shapes rule viability, while institutional adaptations feed back into agent incentives and perceptions of legitimacy.

Level	Process	Emergent trust feedback	Effect on system
Micro	Validators respond to incentive structures and reputation signals.	Honest behaviour accumulates and feeds into meso-level rule validation.	Enhanced individual compliance reduces need for external enforcement.
Meso	Coordination rules adapt based on observed agent behaviour.	Rule legitimacy is reinforced or eroded by aggregated trust outcomes.	Institutional cost structure adjusts; scalable governance emerges.

Table 6 - Micro–Meso trust dynamics

This framework addresses a theoretical gap in the literature: rather than postulating organizational trust as an exogenous condition, it demonstrates how trust emerges endogenously from incentive-compatible interactions and consistent behavioural feedback. Decentralized architectures are thus reinterpreted: not merely as technical infrastructures, but as institutional mechanisms for trust generation and reinforcement. Trust is no longer assumed but is produced, stabilized, and scaled through micro-meso feedback loops.

3.4 Discussion: blockchain as institutional technology

Blockchain challenges traditional views of innovation by functioning not just as a General-Purpose Technology (GPT), but as a distinct institutional technology. Unlike typical GPT, which lowers costs of inputs or processing, blockchain reconfigures coordination and trust through cryptographic consensus and protocol-based enforcement. These features can replace roles once held by legal or hierarchical systems, reducing transaction costs tied to verification, enforcement, and monitoring. While it shares core GPT traits - such as adaptability and capacity for complementary innovation (Kane, 2017) - blockchain uniquely embeds governance and incentives in its architecture, forming a new kind of “institutional technology” (Davidson et al., 2018).

Considered through modern institutional economics, blockchain replaces centralized or relational trust with algorithmic certainty. Smart contracts and decentralized ledgers enable coordination without intermediaries, reshaping the mix of market, firm, and hybrid governance. As (Berg et al., 2019) argue, this “industrializes trust”, shifting it from legal or social domains into technological design. The result is not just efficiency gains, but a new institutional paradigm where protocol replaces authority.

The model presented in this chapter reinforces this hypothesis. The meso-level highlights reduced enforcement costs and novel coordination, while the micro-level shows how these emerge endogenously. Validators respond to smart contract incentives, and their aggregated actions generate institutional trust over time. This endogenous trust both limits enforcement needs and aligns behaviour with systemic goals. Blockchain thus serves not only as infrastructure, but as a constitutive force in governance, shaping actions and producing institutional outcomes.

Cryptographic consensus closely mirrors organizational governance: like contracts or incentive schemes, it aligns individual behaviour with collective goals. This analogy reveals the value of economic theory in understanding how decentralized systems coordinate self-interested agents without hierarchy.

Such alignment challenges traditional notions of firm boundaries. If, as (Coase, 1937) argued, firms arise to minimize market transaction costs, then blockchain - by automating search, contracting, and enforcement - undermines that rationale. Reliable external coordination becomes feasible, allowing firms to externalize operations while retaining control over strategy and design. Economic activity thus becomes more modular, and the line between internal and external governance blurs, as blockchain-enabled networks replicate internal coordination features - uniform rules, aligned incentives, and low oversight - without requiring integration.

Blockchain transforms governance by replacing vertical, authority-driven compliance with horizontal, protocol-based enforcement. Misconduct triggers automatic penalties, shifting from discretionary to deterministic rule execution. While this enhances consistency, it also limits adaptability, smart contracts struggle with exceptions and rigidity. To address this, hybrid models are emerging, blending code with flexible mechanisms such as upgradeable contracts, community governance, and legal safeguards (Shah, 2024). These hybrids suggest future organizations may integrate algorithmic control with human oversight.

Blockchain introduces a different coordination logic: decentralized, rule-based, and firm-like in reliability, yet without formal hierarchy. It removes internal agency layers, reduces market frictions, and enables scalable, anonymous cooperation through shared protocols.

This logic is exemplified by V-form organization. Here, smart contracts replace management, and cryptoeconomic incentives ensure alignment. Cohesion arises from protocol, not control. Yet, the viability of V-Form organizational designs is conditional on the maturity of the surrounding blockchain infrastructure, technical reliability and scalability, governance mechanisms for upgrades and dispute resolution, and regulatory recognition and compliance toolkits. Because these conditions are still uneven and, in many jurisdictions, under development, V-Form structures are currently more likely to emerge as modular “overlay” arrangements that complement existing U-Form, M-Form, and VO architectures for selected coordination tasks, rather than as wholesale replacements of established organizational forms.

Blockchain as an institutional technology redefines trust, coordination, and governance. This study showed how it links micro-level incentives with meso-organizational outcomes, enabling new ways of organizing that embed trust in code and make firm boundaries more fluid.

3.5 Conclusions

This chapter develops a multi-level framework to analyse how the implementation of blockchain can reshape organizational forms. By examining the shift between different organizational forms, it shows how technology, economics, and institutions co-evolve to redefine cost and governance dynamics.

At the meso level, organizations are seen as rule systems balancing coordination and trust costs. Hierarchical models like U-form and M-form reduced trust costs via internal authority but struggled with coordination as complexity grew. Networked organizations improved flexibility but incurred high trust costs without strong relational or legal safeguards. The blockchain-enabled V-form offers a new solution: it minimizes both coordination and trust costs through decentralized protocols that embed consensus, enforcement, and reputation mechanisms. This enables scalable cooperation without centralized control.

To deepen this analysis, a micro-level model explores validator behaviour under smart-contract-based governance. The model shows that when incentives align with protocol integrity, honest behaviour becomes a stable strategy. This generates endogenous trust that scales over time, reinforcing organizational efficiency at the meso level. By linking behavioural dynamics with structural outcomes, the model addresses a key limitation of conventional theories: it explains how trust is not assumed or imposed but produced through incentive-compatible interaction within decentralized systems.

This multilevel framework advances theory and practice by reframing blockchain as an institutional substrate, not merely a technological tool. It endogenizes trust and links micro-level behaviour to meso-level outcomes, offering a dynamic alternative to static transaction-cost models. Practically, it informs firms and policymakers on transitioning from internal coordination to decentralized collaboration and clarifies the institutional logic of emerging entities like DAOs and consortia.

The interdisciplinary approach is central. It recasts technical concepts such as consensus protocols through economic theory, enhancing our understanding of blockchain governance and offering organizational insights for designing distributed systems. Consensus design carries structural consequences: proof-based systems foster competitive dynamics, while vote-based models support collaborative governance. These choices map onto distinct agency environments, influencing trade-offs between decentralization, efficiency, and control.

This framing supports practical evaluation: it helps determine when blockchain governance is preferable and anticipates regulatory challenges posed by blockchain-native organizations. A key issue is the contrast between endogenous and exogenous trust enforcement. In permissionless systems, incentives internalize trust through protocol-level alignment. In permissioned settings, trust relies more on external governance, leaving systems vulnerable to free-riding, collusion, and misaligned incentives. Such vulnerabilities are heightened when

organizational-level rewards fail to motivate individual validators. Ensuring alignment in these contexts remains unresolved. A promising direction is the integration of contract theory into blockchain governance, a research path already underway and critical to the evolution of future protocol models.

This analysis, while based on stylized models, highlights the need for empirical testing across blockchain ecosystems to validate and refine its claims. Its core insight is that blockchain transforms coordination by enabling modular, less hierarchical organizations governed by transparent protocols rather than authority or trust-based relationships. In doing so, it overcomes the trust limitations that constrained earlier virtual organization models, not only lowering governance costs but reshaping how cooperation is structured and incentivized.

Organizational evolution, then, is not a linear replacement of forms but an adaptive process driven by shifts in institutional technologies. Blockchain represents such a shift, enabling new forms like the V-form and providing the infrastructure to scale them. By linking micro-level incentives with meso-level governance, this framework allows for a deeper understanding of both the trajectory and mechanisms of organizational change.

3.6 Future insights

The proposed micro–meso framework opens several research insights. As blockchain-based forms like the V-form evolve, their influence may extend from firms to macro-level structures, especially in transparency-driven sectors. Studying such ecosystems requires models addressing institutional co-evolution, systemic risk, and inter-protocol dependencies.

Hybrid organizations, blending hierarchy and protocol coordination, raise questions about governance interoperability, legal alignment, and decision rights. Key challenges include DAO performance, participation, incentive sustainability, and adaptability. Behavioural models grounded in evolutionary dynamics could help assess their long-term viability.

The resilience of decentralized systems also warrants analysis. While assumed to absorb shocks better, actual robustness may hinge on modularity and protocol coupling. Loosely coupled networks might contain failures, whereas shared protocols could amplify them. Complexity theory and systems modelling can clarify whether such structures are genuinely antifragile or merely decentralized in form.

Permissioned networks present further challenges. When validators are organizations, misaligned incentives can lead to shirking or bribery, compromising system integrity (Auer et al., 2021). Designing effective, incentive-compatible governance for such environments demands a fusion of blockchain engineering and contract theory. Tackling validator free-riding, collusion, and accountability will be essential as enterprise consortia grow and decentralized infrastructure becomes critical in sectors like finance, logistics, and public services.

The rise of blockchain as an institutional technology is likely to reshape macro-institutional frameworks (Berg et al., 2019). As DAOs and decentralized consortia gain economic relevance, legal and regulatory systems must adapt. While some jurisdictions are experimenting with DAO recognition, key issues (liability, taxation, and dispute resolution) remain unresolved. The

interaction between formal institutions and protocol-based governance will influence the legitimacy and scalability of these new forms, potentially giving rise to a meso-institutional layer ensuring interoperability with existing systems.

This framework can also be applied to other technologies with decentralized principal–agent dynamics. AI alignment challenges, for example, resemble classic agency problems where incentives must be embedded in system design (Hadfield-Menell, 2021). Similarly, DeFi platforms face governance issues like vote concentration and low participation (Barbureau et al., 2023). Comparative analysis across domains like AI and DeFi can reveal shared principles of incentive alignment and distributed governance.

The multi-level framework developed offers a foundation for exploring emerging models of coordination. V-form is likely a transitional phase in organizational evolution, enabling experimentation with distributed governance and institutional innovation. As decentralization advances, new hybrids and challenges will emerge. This framework provides tools for understanding and guiding this transformation.

CHAPTER 4

Blockchain as economic infrastructure: incentives and governance mechanisms

Following the development of the V-Form organizational model in Chapter 3, which proposes a novel blockchain-based organizational structure, the thesis then turns to the technological foundations needed to support such forms.

In the Chapter 4,⁷ the focus shifts from organizational design to the rules enabling decentralized coordination, specifically through an analysis of blockchain's core consensus mechanisms viewed through the lens of economic governance.

Consensus algorithms - such as Proof of Work, Proof of Stake, and Byzantine Fault Tolerance - are presented not merely as technical procedures for achieving agreement in distributed networks, but as institutional arrangements in their own right. By connecting concepts from computer science with themes in institutional economics and agency theory, this section of the thesis provides an interdisciplinary understanding of how consensus protocols act as embedded governance rules. They coordinate behaviour, manage incentives, and ensure compliance among participants much like contracts or regulations in traditional organizations. This comparative examination complements the earlier discussion: whereas the previous section introduces the conceptual model of decentralized organizational forms, the next explores the technical-economic mechanisms that make them operational. The progression thus moves from theorizing new structures to analysing the protocol-level governance systems that render decentralized organizations feasible.

4.1 Introduction

Blockchain technologies are increasingly analysed for their potential to reshape organisational structures and governance models, as well as for the implications they have on traditional systems of coordination and control (Berg et al., 2019). This chapter aims to bridge the gap between economics and computer science by reinterpreting key technological concepts - such as consensus protocols - through the lens of economic theory. In doing so, it seems that blockchain governance mechanisms can be more effectively understood through the lens of agency theory, yielding valuable insights for both fields.

⁷ An earlier version of this chapter was presented as a conference paper: Murano, A., Bruno, B., Vespri, V. (2025), *Blockchain as Economic Infrastructure: From GPT to Institutional Technology – An Analysis of Incentives and Governance Mechanisms*, CIBES Conference, Prague, 19–21 June 2025. The proceedings are forthcoming in the volume *Shaping the Future of Business and Economics: Innovation, Transformation, and Global Impact*, published in Springer Proceedings in Business and Economics.

This analysis moves beyond the conventional debate on blockchain applications to position it within the broader category of General Purpose Technologies (GPTs). Just like historical technological revolutions - such as the steam engine, electricity, computers, and the internet - blockchain possesses the fundamental characteristics of a GPT: pervasiveness, continuous improvement, and the capacity to generate complementary innovations. Yet, its unique features also challenge traditional economic assumptions regarding agency problems in technological adoption.

From an economic standpoint, a GPT should not inherently generate an agency problem (Allen et al., 2023) since, as argued by (O. Williamson, 1985; O. E. Williamson, 1975), machines are not opportunistic. However, blockchain presents a unique case where governance mechanisms must be explicitly designed to align incentives among participants. By integrating insights from cryptographic consensus mechanisms into agency theory, this section offers an interdisciplinary approach that enhances the understanding of both the technological infrastructure (blockchain as a system) and the governance models of decentralized organizations, such as Decentralized Autonomous Organization (DAO), that is a code-governed structure designed to operate without centralized control (Wang et al., 2019).

This dual perspective is particularly relevant when analysing consensus protocols, which not only secure the network but also shape its organizational structure. Proof-based mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), align with competitive organizational models that emphasize individual incentives and rivalry among validators. In contrast, voting-based mechanisms, such as Practical Byzantine Fault Tolerance (PBFT), resemble collaborative structures where decisions emerge from collective agreement rather than individual competition. Reframing these mechanisms through an economic lens highlights their role in balancing organizational incentives and efficiency trade-offs, offering a more structured understanding of blockchain governance.

A central question in this regard concerns the governance mechanisms embedded within blockchain networks. Unlike traditional hierarchical organizations, blockchain operates through decentralized structures in which nodes play an active role in validating transactions and maintaining network integrity. This raises a key agency dilemma: how can a system lacking centralized control ensure that individual participants act in alignment with the network's objectives?

To address this, blockchain governance through the lens of the principal-agent problem is reinterpreted, where the blockchain itself functions as the principal, and the network nodes (validators, miners, or participants) act as agents. The blockchain's objective is to ensure system reliability and efficiency, while agents seek to maximize their individual payoffs. The nature of this agency relationship depends on the blockchain's governance structure, differing substantially between permissionless and permissioned models. In permissionless blockchains, incentives are embedded directly in the protocol, aligning agent behaviour through cryptographic rewards. In contrast, permissioned blockchains require external governance mechanisms to regulate validator actions. This is particularly evident in

permissioned blockchains, where validators often operate within organizational settings. In consortium blockchains, for example, validators may be employees of participating firms, leading to potential misalignments between individual incentives and organizational objectives. While transaction fees and rewards are typically assigned to the organization, the individual validator's effort and resource consumption (e.g., computational power and labour) may not be directly linked to personal benefits, introducing a classic principal-agent dilemma. Blockchain meets all the criteria set by (Bekar et al., 2018) for a GPT, suggesting a wide range of potential applications, from financial services and healthcare to public administration and trade (Berg et al., 2019). By analysing blockchain through an interdisciplinary approach, we highlight how economic models can provide new tools for understanding decentralized governance structures. This perspective enhances both economic theory and the technical understanding of blockchain, positioning it as more than just a financial innovation but as a governance mechanism for digital and organizational ecosystems.

A key distinction in blockchain governance lies in how different architectures manage incentives and control mechanisms. While permissionless blockchains rely on cryptographic incentives to align self-interested behaviour with system objectives, permissioned blockchains require external governance mechanisms - such as contractual agreements - to regulate validator behaviour. Designing these contracts effectively remains a challenge, particularly in addressing asymmetric information and external incentives (e.g., corruption). By integrating economic theory with blockchain governance analysis, this study offers a structured approach to these unresolved issues.

The economic approach to blockchain functioning and features offers valuable insights to the extensive body of literature that has primarily emerged from computer science. Economics approaches problem choices differently from hypotheses and objectives employed in computer science investigations. In computer science, researchers classify agents as honest and faulty, showing that blockchain will succeed if no more than a given percentage of agents are faulty. In contrast, the economic perspective - particularly in game theory - seeks to establish equilibrium conditions in which no agent has an incentive to deviate from a given strategy (Abraham et al., 2006). This fundamental difference stems from the fact that computer scientists typically assume agent behaviour based on predefined categories - where “an honest node behaves honestly, while a faulty node always misbehaves” (Chen et al., 2020) - whereas economists assume self-interested agents and derive behaviour from individual utility functions.

Furthermore, (Amoussou-Guenou et al., 2023) emphasize the divergence between computer science and economic traditions in modelling individual behaviour, highlighting that game theory assumes all players (or processes) to be rational, whereas computer science differentiates between correct processes that adhere to the protocol and those that may behave arbitrarily or maliciously.

These differing assumptions have profound implications for governance models in blockchain networks. The governance structure embedded in a blockchain determines the nature of the agency relationship between the system (as principal) and its nodes (as agents). In permissionless blockchains, decentralization is achieved through cryptographic incentives,

where participation is open to any agent who satisfies the protocol's conditions. Here, consensus mechanisms act as self-enforcing contracts, aligning agents' incentives without the need for external enforcement. In contrast, permissioned blockchains introduce additional governance layers, where participation is restricted to pre-approved entities, often requiring contractual agreements or hierarchical control mechanisms to address agency issues.

The role of consensus protocols is particularly relevant in shaping the principal-agent dynamics within blockchain networks. Vote-based consensus mechanisms, such as Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA), illustrate how the degree of decentralization affects the nature of the agency problem. In PBFT, for instance, a system can tolerate up to one-third of malfunctioning or malicious nodes while maintaining network security through a combination of cryptographic validation and majority agreement. However, validators play an active role in the communication and verification process, which introduces potential moral hazard problems. Since verification effort is not always observable, validators may exert suboptimal effort unless properly incentivized, highlighting the need for differentiated contract structures to mitigate hidden-action risks.

Different assumptions lead to different research objectives. Computer science primarily investigates conditions for the effective functioning of technological instruments, including the impact of voluntary and involuntary deviations from expected behaviour. Economists, on the other hand, focus on how and why individuals and organizations adopt technologies, analysing the effects of innovation on the economy, the differential spread of innovation across sectors and countries, and the challenges and barriers to technology adoption. A comprehensive framework must consider not only the interaction between human agents and technology but also the interactions among human agents mediated by technology.

The adoption of blockchain varies significantly across economic sectors. According to (Grover et al., 2019), finance, insurance, and real estate industries have reached the confirmation stage of the innovation-decision process, while sectors such as transportation, communications, utilities, and trade remain at the decision stage. Manufacturing is still in the knowledge stage, whereas public administration has only reached the persuasion stage. This variation underscores the role of economic analysis in understanding the structural factors influencing blockchain adoption, including institutional, regulatory, and behavioural aspects. Moreover, the design of contractual incentives in permissioned blockchains remains an underexplored area, particularly regarding external incentives, enforcement mechanisms, and the potential risks of corruption in validator selection.

This chapter analyses blockchain through an economic lens, considering it both as a production technology and as a governance system for firms and organizations. The primary focus is on the differences between private and public blockchains and the consequent governance implications for labour relationships. The agency problem inherent in blockchain governance can be analysed through the lens of contract theory, particularly in permissioned blockchains, where incentive structures play a critical role in ensuring compliance and efficiency. Thus, this study not only deepens the understanding of blockchain's economic impact but also provides a structured framework that can be used to refine governance mechanisms in decentralized and permissioned blockchain ecosystems.

The chapter is structured as follows. In Section 4.2, the main structural characteristics of blockchain are explored, to highlight the differences between private and public blockchain architectures and their implications for governance. Section 4.3 examines the mechanisms that regulate relationships within blockchain systems, particularly in the context of agency theory. Section 4.4 focuses on asymmetric information in permissioned blockchains. Section 4.5 concludes with insights on open questions and a research agenda.

4.2 Principal-Agent Dynamics in Blockchain Platforms

Starting from the interdisciplinary perspective just introduced, this section explores how agency theory can provide a structured framework for analysing governance in blockchain platforms. While governance mechanisms are discussed in detail in the next section, here the focus is on the principal-agent relationship as a foundation for understanding incentive structures and decision-making processes in different blockchain architectures. By framing blockchain governance through the lens of agency theory, it is highlighted how different blockchain models (permissionless and permissioned) manage trust, control, and incentives. Expanding on the broader issue of designing incentive mechanisms within the blockchain economy, as outlined by (Beck, 2018), a specific problem and proposed solution through the lens of agency theory (Eisenhardt, 1989) is conceptualized. This methodological choice enables to examine the implications of this study for incentive structures in permissioned blockchains. This analysis serves as an initial step toward understanding the underlying mechanisms that govern incentive systems in such environments.

Agency theory highlights two core issues in contractual relationships: adverse selection (Akerlof, 1978) and moral hazard (Arrow, 1963). These problems stem from asymmetric information between the principal and the agent, leading to misaligned incentives within blockchain ecosystems (Beck, 2018). To address these challenges, we incorporate concepts from agency theory (Spence, M., 1973), along with blockchain-specific incentive mechanisms (Okada et al., 2017), to develop an effective framework for incentive design.

An agency relationship emerges when one party (the agent) acts on behalf of another (the principal), a dynamic present in nearly all contractual agreements (Ross, 1973). However, two significant challenges arise within this framework (Eisenhardt, 1989): (i) a divergence in objectives between the principal and the agent, and (ii) the principal's inability to fully observe the agent's behaviour. The presence of asymmetric information exacerbates these challenges, leading to deviations from traditional economic assumptions based on perfect information. Due to these informational constraints, agents operate under bounded rationality rather than complete rationality (Ross, 1973).

When applied to blockchain networks, the principal-agent relationship differs based on the governance model adopted. In permissionless blockchains, governance is embedded in the protocol itself, relying on cryptographic incentives and economic rewards to align agent behaviour with system objectives. Here, the agency problem is mitigated through decentralized

consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS), which establish self-enforcing contracts where agents' incentives are naturally aligned with the principal's goal of network security and transaction validation. Conversely, in permissioned blockchains, governance involves external oversight and contractual agreements that regulate validator behaviour. These differences in governance affect the intensity and nature of agency problems, particularly concerning monitoring and enforcement mechanisms.

Deepening the framework, moral hazard occurs when an agent, having control over hidden actions or possessing undisclosed information (Hart, 1986), fails to exert optimal effort, ultimately harming the principal's interests. Conversely, adverse selection (Rothschild & Stiglitz, 1976) arises when an agent misrepresents their qualifications or attributes, leading the principal to make suboptimal choices. A well-known illustration is the "market for lemons" (Akerlof, 1978), where uncertainty about quality distorts market outcomes. This theory is a foundational concept in economics that explains how information asymmetry between buyers and sellers can lead to market failure, particularly in markets where product quality is difficult to observe before purchase.

When a blockchain platform is modelled as the principal, intriguing implications arise, given that the platform consists of both organizations and stakeholders who simultaneously act as agents. A fundamental distinction must be acknowledged: while these entities serve as agents pursuing individual interests, they collectively form the principal through the blockchain community's governance structure. This duality allows them to implement incentives and regulatory mechanisms that align individual behaviours with the broader interests of the platform.

Blockchain's role as a governance structure influences how these problems manifest. In permissionless blockchains, self-interested agents (e.g., miners or validators) autonomously choose whether to participate in the consensus process, accepting the incentives and costs embedded in the protocol. This results in a market-driven governance model where cryptoeconomic incentives replace traditional principal-agent controls. However, in permissioned blockchains, where participation is restricted, governance structures must introduce additional contractual mechanisms to align agent behaviour with the principal's objectives, increasing the need for external enforcement mechanisms. The implications of these governance differences are further explored in the next section, where blockchain's organizational structures and performance trade-offs are analysed.

This framework results in an overlap between principal and agent roles, differentiated only by specific contexts. While some might argue that this scenario does not conform to a conventional agency relationship, we sustain that it does, as it meets the conditions specified by (Eisenhardt, 1989): (i) individual agents pursue divergent objectives, and (ii) the community lacks comprehensive oversight to monitor each participant's actions. Moreover, since individual agents have incentives to obscure their behaviours from the broader community, governance mechanisms must be designed to counteract these tendencies.

The literature identifies three primary agency problems that contribute to agency costs (Kraakman et al., 2017):

- i. *Vertical Agency Problem*. This arises in relationships between principals (shareholders) and agents (managers). In traditional corporations, managers may prioritize personal objectives over maximizing shareholder value.
- ii. *Horizontal Agency Problem*. This occurs between majority and minority shareholders. Majority shareholders (agents) may exploit their voting power to extract private benefits at the expense of minority shareholders (principals).
- iii. *Firm-Stakeholder Agency Problem*: In this scenario, the firm (agent) may leverage its position opportunistically, prioritizing its own interests to the detriment of stakeholders such as employees and consumers (principals).

These issues become particularly pronounced when principals are dispersed and heterogeneous, as they encounter difficulties in information collection and coordination (Spear, 2004). The absence of trust further intensifies these challenges, underscoring the necessity of governance mechanisms to mitigate them.

Agency problems are not exclusive to conventional corporate structures; they also manifest in worker cooperatives and DAOs. In cooperatives, members' interests extend beyond financial considerations to include social and utility-based objectives, introducing distinct governance challenges. Governance structures must accommodate these varied interests, especially in organizations that follow a "one member, one vote" model, where horizontal agency issues emerge due to preference diversity (Spear, 2004). For example, disparities between senior and junior members regarding tenure and priorities can hinder decision-making and lead to misalignment (Basterretxea et al., 2022).

In the context of blockchain, DAOs provide a unique case study for examining how agency problems evolve in decentralized governance models. Unlike traditional organizations, DAOs rely on smart contracts and token-based voting mechanisms to enforce governance rules, reducing reliance on external enforcement. However, DAOs are not immune to agency problems: majority token holders may exert disproportionate influence over decision-making, creating horizontal agency problems similar to those in traditional shareholder structures. These governance issues underscore the importance of designing incentive-compatible mechanisms that balance decentralization with effective decision-making, a theme further developed in Section 4 through an analysis of consensus protocols.

Although agency theory remains a contested framework for governance analysis, it continues to influence both corporate and blockchain-based organizational models (Kaal, 2020; Michaud & Audebrand, 2022). The primary goal of effective corporate governance is to mitigate these agency costs (Pargendler, 2016).

To address agency costs, organizations are increasingly adopting a governance-by-design approach (Mannan, 2023). This strategy integrates both technical and legal governance tools, such as smart contracts and operational agreements, to proactively mitigate agency issues. In DAOs, governance-by-design aims to eliminate agency costs ex-ante by embedding these mechanisms within their governance frameworks.

4.2.1 Blockchain governance structures and performances

Blockchain (BC) technology, originally developed for cryptocurrencies like Bitcoin, is now explored also for non-cryptocurrency applications. BC are usually categorized in: permissionless, and permissioned. Permissioned BC can be categorized into private BCs, consisting of one server and multiple users, and consortium BCs, which are groups of private BCs.

While permissionless BCs are the basis of the cryptocurrency markets and may diffuse across both individuals and institutions, permissioned BCs are more interesting for organizations and institutions whose concern is the diffusion among firms or offices rather than among individuals (Helliard et al., 2020).

Permissionless BC refers to a type of blockchain where anyone can participate in the network without requiring permission. It is a decentralized and open system that allows anyone to join, validate transactions, and create new blocks. The most known example of permissionless BC is Bitcoin, which is also the origin of the technology itself. Well-known examples of permissionless BCs are Bitcoin and Ethereum.

On the other hand, permissioned blockchain refers to a type of BC where users are verified and approved before participating in the network. Participant will be whitelisted or blacklisted with some type of procedure (Swanson, 2015). Permissioned BCs provide customizable rules for participation and operation (e.g., roles and permissions for different users). It can be seen as the favourite solution to federate companies or organizations to manage economic or administrative interactions. Permissioned BCs are usually non-cryptocurrency, because they allow control over who can join and interact with the network, which is often fundamental for business or enterprise use cases. Hyperledger Fabric for enterprise solutions is a well-established example of permissioned BC.

Permissioned BCs can be classified into private and consortium models. In a private BC, a single entity governs the system, maintaining central control while distributing data across multiple nodes (Dib et al., 2018). Consortium BCs represent a collaborative framework where multiple organizations share control over a distributed ledger. Consortium BC is a type of BC that supports a network where participants can be limited to a subset of users and data access is strictly controlled. It allows users holding the same access licenses to the BC system, even if they belong to different organizations.

Beyond these descriptive characterizations of different types of BCs, it is of interest for the present study to enlighten the principal differences between permissionless and permissioned BCs in terms of production process and organizational structure.

From an organizational perspective, BCs can be seen as networks of nodes that either collaborate or compete to generate an immutable sequence of verified transactions. On the other hand, from a technological standpoint, BC defines how each node combines various inputs - such as human labour, computational power, and storage capacity - to generate a functional distributed ledger. The two technologies available (permissionless and permissioned BCs), imply different combinations and substitution degrees among inputs (basically labour and capital). The technology itself dictates the different role inputs assume in the production process, and particularly how much intensive can be the effects of individual actions and choices on the output results. Because of the different intensity of human action,

the two technologies imply also different governance systems, because human beings can be differently involved in BCs performances. Technological characteristics of BCs production functions concern the way labour and capital are managed by each node to produce the final output, whereas the organizational structure concerns the degrees of freedom each node has in combining inputs.

This study explores the answers to the following research questions.

RQ1. Which are the main elements of BCs fully describing the production function technology?

RQ2. How different BCs technologies impact the output and which metrics are available to measure output?

RQ3. How different BCs technologies shape the emerging governance system?

The discussion that follows compares the basic configurations of the two blockchain types, emphasizing the technological and structural differences that influence the inputs each system employs. The discussion is based on the concept of “trust”, as a basic architectural prerequisite of these systems. Thereafter, the output dimension of BCs will be consequently discussed, to further refine the agency problem description that characterize the two BC structures.

4.2.3 BC structure and the concept of trust

Permissioned BC require legal identities behind the nodes participating to the validation process, whereas permissionless technologies have pseudonymous and anonymous nodes freely interacting in the validation process (Swanson, 2015). From this characteristics, one can derive a first fundamental foundational structural difference between permissioned and permissionless BCs, concerning how trust is built inside the BC. Nakamoto introduced the concept of trust in blockchain systems through Bitcoin, emphasizing how decentralized consensus can replace traditional trust mechanisms (Nakamoto, 2008). In the computer science perspective, trust relates to how the system ensures integrity, fairness, and resistance to manipulation (Artz & Gil, 2007). In the agency problem, trust is the degree of freedom the principal grants to the agent, based on the contractual refinements or on personal beliefs (Lukas & Schöndube, 2012). In permissionless BCs, trust is inherent in the system design, as the principal has designed the system to grant the maximum degree of freedom to carry out the task assigned (the validation process). As to trust among agents, it is eliminated among participants and replaced with trust in the system (protocols and incentives), so that many authors define this kind of system as trustless. Economically speaking, this mechanism resembles an "invisible hand" where incentives naturally align participants' actions with the system's goals.

In permissioned BCs, trust is centralized at the entry point (trusted validators) and reinforced through external governance. The permissioned BCs are reliant on legal institutions, smart contracts or other external mechanisms who can decide – off-chain - which identities can participate to the system. A central authority (or consortium) admits and authenticates validators, assuming their honesty. Trust among validators is not inherently necessary, as their

identities are known, and external mechanisms enforce accountability. External agreements (e.g., legal contracts, governance frameworks) reinforce trust and provide recourse in case of malicious behaviour. To give a synthetic definition, one can describe this trust model as an out-built trust model.

4.2.4 BC performance output

In the idea of Nakamoto (Nakamoto, 2008), the blockchain project has the aim to build a system pursuing high efficiency in a highly decentralized governance structure.

Simplifying, it is possible to describe the performance of a BC in terms of two main output indicators: efficiency and decentralization. Efficiency and decentralization serve as outcome metrics for evaluating the performance of a BC. Decentralization refers to the degree to which power and control are distributed among participants in the BC. A fully decentralized system allows anyone to participate without central authority. Efficiency reflects the speed, scalability, and cost-effectiveness of the BC. It includes metrics such as transaction throughput, latency, and resource usage. Each structure described before has different output indicators of performance. More precisely, one can describe the relationship between decentralization and efficiency as a typical trade-off in the desired output, and it is the BC's trust model that dictates how decentralization and efficiency trade-offs are managed. Public BCs, where achieving consensus involves many participants, trustlessness allows for highly decentralized structures. This leads to slower transaction times and higher resource consumption, reducing efficiency. Permissioned BCs, involving fewer participants, have higher efficiency at the cost of reduced decentralization, because the trust mechanism is centralized at the entry point and reinforced through external governance.

The description of different BC technologies and their main properties is synthetized in Figure 6, where the panel 1 represent the potential answers to RQ1 and RQ2, whereas panel 2 specify the answer to RQ3.

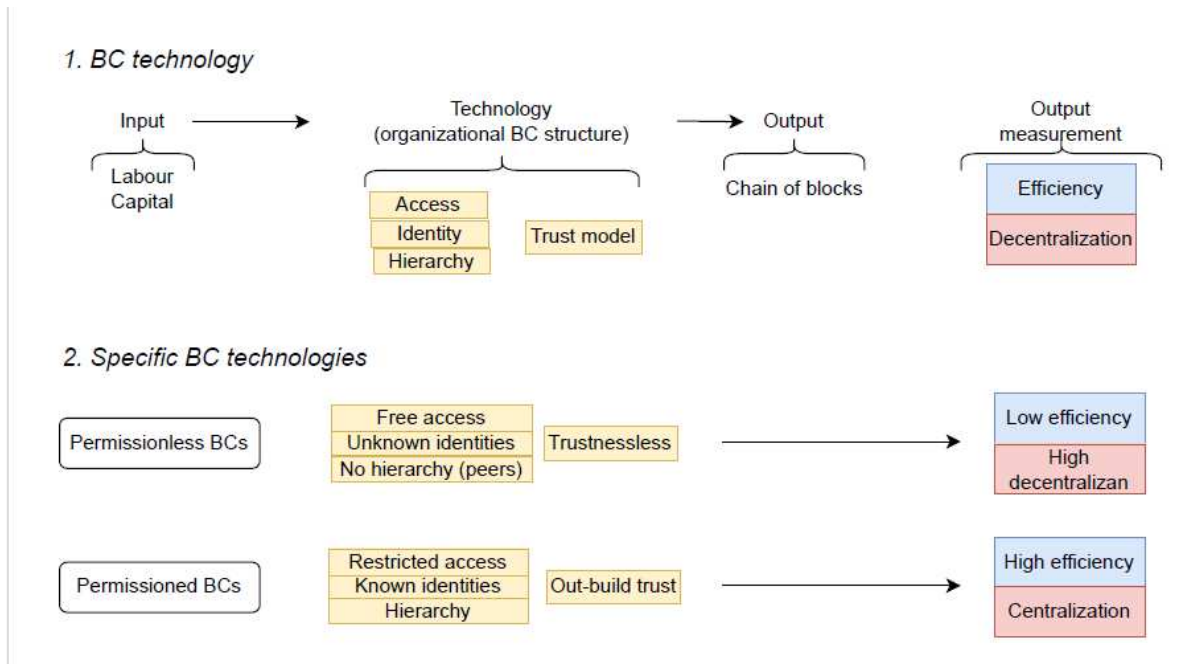


Figure 6 – BC technologies: description and properties

4.3 The agency problem and the consensus protocols

The two basic structures of BC have different implications in terms of the relationship between the principal and the agents, but some common features can be identified.

In this framework, the blockchain acts as the principal, while the nodes function as agents. The principal's goal is to ensure a properly functioning system where blocks are validated and added in a structured process. This validation task is delegated to the nodes. The objective of the nodes is to maximize the net benefit they can derive from the activity of validation, because the activity of validation implies implicit or explicit costs and benefits. The mandate problem between principal and agent depends on the governance structure the BC uses, being the validation mechanism (and its relative benefits and costs), and the governance structure different in permissionless and permissioned BCs. For all kinds of BC a fundamental question concerns “how can record-keeping be designed to incentivize honest reporting” (Abadi & Brunnermeier, 2018).

The different governance mechanisms between permissionless and permissioned BCs imply different relationship in the agency problem. With extreme simplification, in the permissionless BC incentivizing contracts are designed inside the BC system, and agents pursue their self-interest by maximizing the net benefit they can gain from the validation procedure, where benefits are usually represented by cryptocurrencies, whereas costs include explicit fixed and variable costs. In the permissioned framework, the agency problem is more like a command-control delegation mechanism, but it is possible to imagine that incentivizing contracts are designed also in this framework.

It is worth to note that permissionless BCs have usually a native cryptocurrency, whereas permissioned BCs are usually non-cryptocurrency applications, but public (permissionless) BCs (though less common) may use non-cryptocurrency applications, particularly when transparency and decentralization are priorities (e.g., public registries or open certifications).

Non-cryptocurrency applications of BC are often private BCs, because public BCs show certain limitations when applied to industrial use cases, lacking of some characteristics that are essential for corporate and administrative applications (Dib et al., 2018).

Coming back to the agency problem, it is now clearer that in permissionless BCs the mechanism design of the principal agent relationship is the BC itself, that is the contract between principal and agent is accepted autonomously by the agent with the access to the BC, who implicitly accepts its functioning rules. This implies a high degree of decentralization, because no more control is needed for principal and agents acts autonomously pursuing their self-interest objectives.

When permissioned BCs are concerned, the contract between principal and agent is external to the BC, and it is stipulated before the access to the BC. This implies a low degree of decentralization, because the contract itself implies control mechanisms on agent behaviours in the BC. This enlightens the need for clear description of the principal agent contract that have to be stipulated prior the entrance to the BC.

To deepen the different agency relationships in BC structures, it is needed to describe the algorithms governing the procedure for adding blocks. These algorithms are synthetized as follows.

4.3.1 The consensus protocols

The consensus protocol is a set of rules and procedures designed in the BC to give the final validation to a block addition to the chain. The consensus protocol is the process in which a majority of nodes agree on the state of a ledger, and guarantee that the state of a ledger is coherent between multiple participating nodes (Swanson, 2015). Though the concept of consensus is not alien to economics, it is much refined when included in the definition of equilibrium, incentive compatibility, and mechanism design (Chen et al., 2020).

Consensus protocols are strictly linked to the trust model governing the BC. Therefore, two main classes of protocols arise from the two trust models characterising permissionless and permissioned BCs. The two classes of consensus protocols are usually distinguished in proof-based and voting-based. In the proof-based algorithms, the nodes compete in showing to the verifying network that they are more qualified than others to the appending work. In the vote-based protocols, all nodes share their validation results on the new block to reach an agreement on it (Nguyen & Kim, 2018). From the organizational point of view, Proof-based protocols align with competitive organizational models due to their focus on individual performance and competition. In contrast, voting-based protocols resemble collaborative structures by emphasizing collective decision-making and shared responsibility (Oyinloye et al., 2021). This categorization intuitively makes it coherent to associate the proof-based protocols to the trustless BCs (permissionless), and the voting-based to the out-built trust (permissioned) BCs.

When cryptocurrency BCs are concerned, the consensus protocol is also the process for selecting the actual node that will add the next block among all the miners, gaining the crypto reward associated to the puzzle resolution (Dib et al., 2018).

In permissioned BCs, where the participants are bounded by strict contractual obligations to behave correctly, the more efficient consensus protocols belongs to the family of Practical Byzantine Fault Tolerance (PBFT), which are voting-based protocols (Sukhwani et al., 2017; Swanson, 2015).

Consider that the consensus protocol should be able to guarantee BC maintenance not only against faulty agents, but also against other kinds of faults. The PBFT relies on the assumption it should be resilient also if some fraction of agents have faulty nodes that fail to communicate (or send wrong messages), simply because computers may be temporarily disconnected from the network or suffer from programming errors (Abadi & Brunnermeier, 2018).

a) *Proof-based consensus protocols*

The basic concept of proof-based consensus algorithm is that among many nodes joining the network, the node that performs sufficient proof will get the right to append a new block to the chain, and receive the reward (Nguyen & Kim, 2018). The reward is therefore a fundamental element for proof-based protocols because it represents the incentive mechanism fostering the validation process in BC. Main proof-based protocols are the Proof-of-Work (PoW) and Proof-of-Stake (PoS) protocols.

Reinterpreting this protocol family in terms of agency problem, the incentivizing contract between principal (BC) and agents (nodes) is the protocol itself, which is inherent to the BC structure and does not need further refinements or external enforcement. The principal has the objective of a well-functioning BC, whereas the nodes have the objective of maximizing the amount of currency they hold, by maximizing the differences between the currency they can gain from winning the competition in creating proofs and the energy and computational effort expenses they must sustain to create proofs. No more design is needed to align the agents' objectives (maximization of crypto-currencies) with the principal objectives (chain maintenance and well-functioning).

Incentive compatibility constraints are widely discussed in the field of cryptocurrency BCs, based on PoW consensus mechanism (Li et al., 2023), and the reward for mining is easily quantified through the crypto currency. An attempt to adapt the theory of distributed consensus from the computer science literature to an economic setting is in (Abadi & Brunnermeier, 2018), who stress that the provision of incentives is the key of their theory, differently from previous work in computer science, where agents are assumed to behave honestly. Interestingly, the authors underline that the consensus framework they elaborate applies to all types of digital ledgers, from centralized ledgers (permissioned) to PoW and PoS BCs (permissionless). (Abadi & Brunnermeier, 2018) describe a consensus mechanism avoiding the double spending problem. The double spending problem occurs when a node A double spends the same currency (messages) to a node B and at the same time to a node C, so that A and B may agree on the first transaction, whereas A and C may agree on the second transaction.

In all cited studies, the representation of a self-interested rational agent is formulated through the definition of a utility function. In some models, the agents' utility functions are common knowledge, whereas in others they are partially known. The problem with assuming given utility

functions is that it's important to design protocols that can handle unanticipated behaviours by individuals who have utilities that are different from those we expect (Abraham et al., 2006).

b) Vote-based consensus protocols

When non-cryptocurrency BCs are concerned the consensus mechanism cannot be assured by the classical consensus protocols used in crypto BCs (PoW and PoS), which need currencies to be implemented. Two additional consensus protocols can be designed: Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority. Both protocols are widely employed in permissioned BCs (De Angelis et al., 2018).

PBFT

PBFT assumes that less than one-third of the nodes can be faulty (f), requiring a minimum of $n = 2f + 1$ nodes to ensure fault tolerance. If $2f + 1$ peers agree on the block transaction, the block is appended as the next block on private ledger (Castro & Liskov, 2002; Sukhwani et al., 2017).

PBFT requires all nodes to be identified, limiting its applicability in public BCs. The PBFT consensus algorithm involves a leader responsible for ordering transactions, and the consensus process consists of three phases. In the first phase, the leader first broadcasts the transaction request (pre-prepare phase). Then, each validator signs and broadcasts a prepare message (prepare phase), and once a sufficient number of prepare messages are received, validators send commit messages (commit phase). To progress through each phase, a node must secure votes from at least two-thirds of the network (Dib et al., 2018; Hasselgren et al., 2020).

PoA

In many non-cryptocurrency BCs the problem of incentive for mining is overcome by employing the Proof-of-Authority, implying that only authorized administrators are allowed to add blocks to the chains (Kamal et al., 2023).

Proof-of-Authority (PoA) is a consensus algorithm that operates with a group of trusted nodes, called authorities, uniquely identified. A majority of these authorities, at least $N/2 + 1$, is assumed to be honest. PoA algorithms use a consensus mechanism where authorities take turns creating blocks in a mining rotation scheme, ensuring fair distribution of block creation responsibilities (De Angelis et al., 2018).

Both types of protocols are based on the full identification of the nodes who participate to the validation process, who are assumed to be honest. The agency problem is externally defined and need contractual/incentivizing agreements between the principal and the agents to re-align the agents' objectives with the principal's ones. It is worth to note that no reward is necessarily linked to the validation effort of the nodes. The validation task is a contractual duty the agent receives in the job description and relies on the original labour contract stipulated.

When coming to non-cryptocurrency BCs, based on PBFT consensus or similar protocols, the continuance and maintenance of the BC also depend on the truth of information that the validator reveals, and to this end the consensus protocol alone is not enough (Li et al., 2023).

Consequently, studies on incentive compatibility for POW are not adaptable to voting-based BCs (Li et al., 2023).

(Abadi & Brunnermeier, 2018) solve the double spending problem in permissioned ledgers by imposing that the centralized authority behaves honestly. “Centralized ledgers tolerate faults in all nodes other than the record-keeper’s” (Abadi & Brunnermeier, 2018). As a whole, the incentive compatibility problem is not fully solved in the permissioned BC.

For PBFT protocols, (Abraham et al., 2006) define resilient Nash equilibria, where rational agents play maximizing self-interest utility functions, and the equilibria are resilient because they tolerate deviation from equilibrium by coalitions of players. The incentive mechanism is an upgrade of the study by (Halpern & Teague, 2004).

An incentive mechanism is also developed in (Amoussou-Guenou et al., 2023) for committee-based BCs, which is a BC where at each height of the BC, a committee is chosen, and one member acts as the proposer, sending a block to the others. Upon receiving the block, committee members decide whether to vote for it, which incurs a cost in energy and computational resources, or abstain, which is cost-free. A block is accepted and added to the BC if it receives a qualified majority of votes. Voting members receive a reward when a block is approved, but endorsing an invalid block results in a cost, reflecting the reputational damage to the BC and its native currency. This process outlines a dynamic game involving strategic decisions based on potential gains and losses. In the described framework, the authors write down the extensive form of the dynamic game, analyse the equilibria of the game, which can be multiple equilibria of a coordination game, and enlightening the existence of free riding problems among opportunistic players.

Interestingly, all proposed game theory approaches are designed in non-cooperative games. An exception is in (Groce et al., 2012), who describe a cooperative game.

Other studies investigate incentive compatibility in PBFT protocols, which can be adopted in non-cryptocurrency BCs. The coin is the basic element of incentive mechanisms for permissionless BCs (Swanson, 2015), but the design suited for public BCs with cryptocurrency may not be ideal for business applications, where the dependency on a specific cryptocurrency could be not preferred (Cachin & Vukolic, 2017).

A detailed discussion of these compatible incentive studies is in (Li et al., 2023), who put in evidence main characteristics and limits of proposed mechanisms.

The authors also show that the consensus mechanism for PBFT is not incentive compatible. They consider three types of agents: Honest (H), Lazy (L) and Malicious (M) validators. In the honest strategy, transactions are validated honestly. In the lazy strategy validators broadcast the validation results without computation, whereas malicious validators (M) intentionally broadcast the validation results as invalid. The honest strategy (H) is always a dominated strategy, resulting in a lower payoff compared to the other two strategies. Intuition is based on the different cost’s validators deal with. Malicious and lazy validator face no verification cost, whereas the honest validator has a positive cost of validation. Lazy nodes are free-riders if they validate blocks without incurring in the relative costs. In this way, they can gain the rewards at the cost of honest contributors. On the other side, honest nodes knowing the free-riding problems can be reluctant to contribute to the network. A public good problem arises. To

overcome the costs asymmetry among players' types, an audit process is added to the protocol to commit punishments to incorrect behaviours (Li et al., 2023).

Finally, (Murano et al., 2024) present a theoretical analysis of the incentive compatibility of two different remuneration schemes for both honest and faulty nodes, demonstrating that one scheme incentivizes honest behaviour, while the other does not.

4.3.2 Costs and rewards

The costs and rewards question in permissioned BCs is a key issue. In some studies, it is assumed that a financial reward exists for validators, because BC validation is a resource consuming process. Furthermore, also reputation rewards are used to encourage the desired behaviours (Li et al., 2023).

As to the costs, some assumptions are often used for all types of BCs. (Catalini & Gans, 2020) categorise costs as networking costs and verification costs (Li et al., 2023). Networking costs include the communication costs among peer nodes, the latency times and bandwidth (Gordon & Catalini, 2018). Verification costs include computation costs as CPU time, hardware, electricity, and other resources consumed during the validation task (Jabbar & Dani, 2020).

Both for costs and rewards, some doubts can arise when applied to permissioned BCs. Let's first consider the rewards. Financial rewards coming from transaction fees cannot always be applied to permissioned BCs. Consider a private/consortium BC with numerous firms/organizations/autonomous entities participating. Nodes can be represented by firms/organizations' employees, who contribute to BC given their corresponding position in the organization. Fees paid for transactions are presumably charged on the belonging organization, as well as the corresponding rewards. Inconsistency between single agent behaviour and organization's objectives may arise.

The same considerations can be applied to the corresponding costs of validation, computation and networking. An agent acting for his principal (the organization) is presumably employing his organization resources (energy, hardware, labour time and so on). Which is the incentive for the single employee to behave by saving costs? It is a standard principal-agent problem that may occur. Incentive compatible contracts must be designed to ensure that the agent choices and actions are aligned with the principal objectives.

4.3.3 BC design and the agency problem

The above discussion has shown the interest for the incentive compatibility problem in consensus protocols. The core element in the agency problem is differently declined in the two families of BCs. In permissionless BCs, the technological characteristics of the production function, previously summarized in the concept of trustlessness, ensure high decentralization, implying that agents find their participation constraint satisfied by having access to the BC. The automatic rules for gaining incentives, through PoW or PoS, solve the incentive compatibility constraint. In permissioned BCs, the agency relationship belongs to the environment outside the BC, and it is often solved in a labour contract describing both incentives and constraints. A

synoptic description of BCs characteristics in terms of principal-agent relationship is in the following table.

		Permissionless	Permissioned
BCs design	Currency	Crypto	Non – crypto
	Incentives	Explicit crypto rewards, explicit costs	Implicit or indirect rewards, external remuneration
	Consensus protocols	Proof-based	Voting-based
Agency contract	Contract timing	At the access to BC	Prior than the access to BC
	Contract type	Incentivizing	Command&Control/ Incentivizing
	External enforcement	None	Yes
	Examples	Bitcoin, Ethereum	Hyperledger Fabric, Quorum

Table 7 - BCs characteristics in terms of principal-agent relationship

4.4 Asymmetric information and governance mechanism in permissioned BCs

The relationship between the principal (the BC) and its agents (validators, miners, and nodes) is shaped by incentive-based contracts, which differ depending on the underlying blockchain structure. Furthermore, in this relationship, asymmetric information may emerge. The occurrence of asymmetric information is particularly relevant for permissioned BCs, where the PBFT protocol relies on the assumption that no more than one third of nodes are faulty.

When an economic perspective of self-interested individuals is adopted, the validity of the PBFT assumptions is strongly weakened, because external incentives may be added to legal enforcements linking principal and agents. Corruption phenomena may undermine the BC functioning, by modifying incentives for one or more nodes belonging to the BC. Literature in the field of information science has analysed some problems that may arise in BC governance, related to corruption, transparency, privacy, and security. A systematic literature review in this field, by (Ibrahimy et al., 2024), identify seven blockchain-based governance models, enlightening that three of them offer anti-corruption solutions, for some specific applications of the BC technology. In the area of management studies, (Trequattrini et al., 2024) perform a similar review of the literature, concluding that the compliance topic is still under investigated.

It still lacks a comprehensive economic approach to contracts design in permissioned BCs, where external incentives and corruption activities can play a role. In a scenario of complete and symmetric information, the agency problem in permissioned BCs can be addressed through external legal contracts that regulate validation tasks. The external contract will provide detailed description of agent duties in the activity of validation. Furthermore, additional incentives can be associated to the activity of validation, as tokens or reputation rewards. These additional incentives can be associated to verifiable and measurable activities of the single validator, as the vote expressed in the validation process. A remuneration scheme can be tailored on positive and/or negative votes expressed by validators. Unfortunately, it could emerge the presence of a hidden action performed by validators. Though the result of validation process is verifiable and measurable, some actions will remain hidden to the principal, creating a potential moral hazard problem.

Simplifying the three phases of the PBFT protocol, it starts with the leader (primary node) proposing a transaction or state update (pre-prepare phase). Validators receiving the message must verify it, sign their agreement, and broadcast it to all the other validators (prepare phase), to indicate agreement with the leader's proposal. In the prepare phase, each validator also receives the prepare messages from the other node. Once the validator verifies that a majority of nodes agree with leader proposal, broadcast commit messages to confirm the agreement (commit phase). After receiving commit messages from the majority of nodes, validator updates its ledger and finalizes the decision.

In this procedure, the PBFT ensures that if no more than one third of the nodes is malfunctioning, the system's resilience arises from a combination of cryptographic techniques and majority agreement among honest nodes. Nevertheless, validators in PBFT play an active role in communication and agreement processes, distinguishing them from passive participants in some other BC designs. In details, each validator assumed to be honest receives a transaction or a state update and verifies the message for correctness and legitimacy. At the end of the verification activity, the validator signs the message and broadcast it to the network. The hidden action the principal cannot monitor is the verification process, that is reading the message and verifying its validity. Though knowing the identities of nodes enhances accountability, each node may be externally incentivized (e.g. with bribes) or intrinsically motivated to reduce his effort in the verification phase. The result is typical labour relationship where the agent performs a hidden action (that is the effort in the verification phase), and the remuneration cannot be directly linked to the unverifiable effort. If the agent does not incur in additional costs for the suboptimal activity performed, the self-interested individual will choose the minimum effort.

By employing the figurative description of PBFT phases usually adopted in information science, Figure 7 details the steps where hidden actions may occur, for both leader and validators. In the figure, the potential hidden actions are coloured in grey.

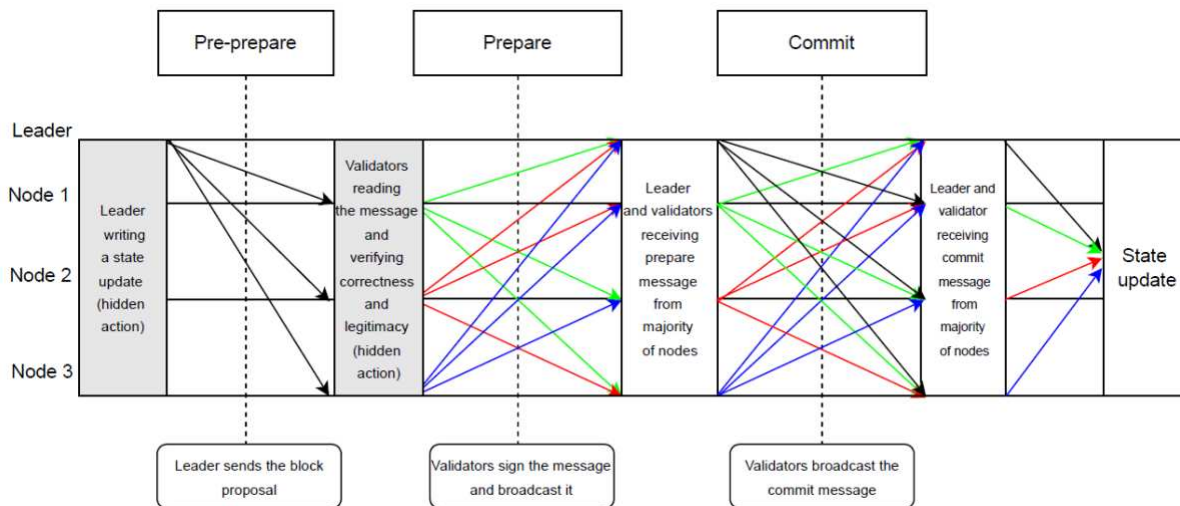


Figure 7 - PBFT phases

In presence of heterogeneous agents, the moral hazard should be treated with differentiated contracts proposals. While in information sciences the honest and malicious nodes are computers that perform in the good or bad way, when coming to an economic perspective, different agent's types matter for their different utility functions and their maximization objectives. Honest nodes can be considered as honest individuals with a specific utility function, different from the malicious node's utility function.

A structured menu of contracts should be evaluated in permissioned BCs, to overcome the moral hazard when heterogeneous agents are involved

4.5 Conclusions

This chapter examined the dynamics of blockchain operation with an innovative governance perspective, focusing on the relationship between consensus mechanisms and the agency problem. By comparing permissionless and permissioned blockchains, the analysis has highlighted how different governance structures shape agent incentives and influence trust mechanisms.

One of the key contributions of this research is its interdisciplinary approach. By reinterpreting computer science concepts (such as consensus protocols) using economic frameworks (such as agency theory), it is possible to generate valuable insights for both disciplines. This perspective not only enhances the economic understanding of blockchain governance but also provides computer scientists with new analytical tools to assess the incentive structures embedded in blockchain protocols. Furthermore, the results suggest that the design of consensus mechanisms has deep implications for organizational structures: proof-based protocols encourage competitive behaviours, while voting-based mechanisms foster collaboration. This connection between technological choices and governance models has significant implications for the efficiency and security of blockchain systems.

The findings indicate that in permissionless blockchains, trust is embedded within the protocol itself, making the agency problem a matter of incentive design through proof-based consensus mechanisms. Conversely, in permissioned blockchains, external governance and legal contracts play a central role in ensuring validator compliance. However, the risk of information asymmetry and free-riding remains more pronounced in permissioned systems compared to fully decentralized ones.

A key challenge in permissioned blockchains concerns the misalignment between individual validator incentives and organizational objectives. When validators are employees of firms or institutions, transaction fees and rewards may accrue to the organization rather than to the individual, leading to potential inefficiencies in effort allocation. Designing incentive-compatible contracts that align validator behaviour with system objectives remains an open issue, particularly in the presence of external incentives such as corruption. Addressing these concerns requires a refined understanding of contract design, which is an area where economic theory can contribute to improving blockchain governance.

This chapter introduces an original methodological approach that leverages economic theory to reinterpret consensus mechanisms. This dual contribution allows to refine understanding of blockchain both as a technological infrastructure and as an organizational model. In particular, by framing consensus protocols as incentive structures within a principal-agent framework, we highlight key trade-offs between decentralization, efficiency, and governance control.

The key contribution of this study lies in its interdisciplinary approach, integrating economic and computer science perspectives to analyse blockchain governance. While prior research has extensively discussed consensus mechanisms from a technical standpoint, this paper provides a structured examination of the agency problem within different blockchain architectures. Such insights are valuable not only for scholars in digital governance but also for policymakers considering regulatory frameworks for blockchain-based systems.

Despite its contributions, there are some limitations. The analysis remains qualitative, and it relies primarily on theoretical frameworks, leaving room for future empirical verification of agent behaviours in various blockchain contexts.

Future research could explore optimal contract designs for permissioned blockchains, particularly strategies to mitigate moral hazard among validators. Moreover, the trade-offs between decentralization, efficiency, and security could be further analysed using quantitative approaches, such as game-theoretic models and economic simulations. Additionally, further work could examine how interdisciplinary approach can be extended beyond blockchain governance to other emerging technologies that exhibit similar principal-agent dynamics, such as AI-driven autonomous systems or decentralized finance (DeFi) protocols.

CHAPTER 5

Incentives for Sustainable Blockchain Governance – A Game-Theoretic Analysis

The previous section's examination of consensus algorithms established that technical mechanisms function as governance tools within blockchain networks. Building on this foundation, the final part of the thesis - summarizing the related scientific paper attached to in the Appendix ⁸- advances the analysis by formally investigating the strategic behaviour of agents operating under these mechanisms.

This section introduces a game-theoretic study that compares different incentive schemes for blockchain validators. Having shown that consensus protocols embed specific rules and incentives, the focus now turns to assessing their effectiveness in practice by modelling validator decisions and potential deviations. The progression thus moves from a broad comparison of protocol designs to a targeted analytical model of incentives and behaviour.

The analysis links the economic notion of incentive compatibility to the operational security of blockchain systems, addressing questions such as:

- *Which reward structures best promote honest participation?*
- *How can penalties or strategic constraints deter attacks?*

By engaging with these issues, the study offers practical insights into how blockchain architectures can be engineered so that individual self-interest aligns with collective objectives. In doing so, the thesis brings together its core themes of technology and institution, demonstrating how rigorous economic modelling can inform the secure and sustainable design of decentralized networks, and providing a conclusion grounded in both theory and application. In the dissertation's overall argument, this chapter serves a specific interpretive function: it provides the micro-foundation for the claim that blockchain can act as an institutional technology only under well-defined conditions. If governance is encoded into protocol rules, then institutional outcomes depend on whether the resulting incentive architecture makes compliant behaviour individually rational for the actors who operate and maintain the network. In the public sector, this in turn requires institutional requirement not only to adopt a platform, but to specify, audit, and iteratively adjust incentive and governance rules over time.

Specifically, Chapter 5 presents a basic game-theoretic analysis of incentive mechanisms in blockchain networks and blockchain-based organizations, with a particular focus on Decentralized Autonomous Organizations (DAOs). This study adopts an economic perspective on blockchain governance, treating network participants (nodes or validators) as rational agents who respond to incentives. By modelling these participants' strategic behaviour, in this

⁸ Bruno, B., Murano, A., & Vespri, V. (2025). Incentives for Sustainable Governance in Blockchain-Based Organizations. Sustainability, 17(21), 9728.

section is examined how different incentive schemes affect both the technical performance (e.g. consensus security, protocol compliance) and the organizational outcomes (e.g. fairness, sustainability) of decentralized systems. The analysis bridges computer science and economics: it not only compares consensus protocols in terms of algorithmic design but also evaluates them as mechanisms to align self-interested behaviour with the collective goals of the network. In extending this inquiry to DAOs, the chapter explores how blockchain-based incentive structures can enable new forms of governance and organizational design. The key findings highlight that well-designed incentives are pivotal for both securing the blockchain network and fostering resilient, equitable forms of decentralized organization. This work has direct relevance for economic and governance design, as it illustrates how careful incentive engineering can shape participant behaviour in ways that support the long-term viability of blockchain ecosystems.

This micro-level focus also clarifies the diagnostic evidence provided earlier. Chapter 1 documented that public organizations face not only technical constraints but persistent skills shortages, unclear governance responsibilities, regulatory ambiguity, and reliance on external vendors. Read through the lens of the present chapter, these barriers are not merely obstacles to implementation: they are constraints on the administration's ability to design and sustain incentive-compatible institutional infrastructures. Where public capability is weak, even technically sophisticated systems may fail to deliver integrity and trust because the equilibrium behaviour of validators and other participants is not aligned with the public objective the system is meant to serve.

From an economic standpoint, blockchain participants can be viewed as self-interested agents with their own preferences and the freedom to deviate if doing so benefits them. Traditional computer science analyses of consensus protocols often dichotomize nodes as “honest” or “malicious” and prove that the system works as long as a certain fraction behave honestly. The economic approach adds nuance by recognizing that agents respond to payoffs: if the rewards for honest behaviour versus cheating are misaligned, even well-intentioned participants might be tempted to free-ride or act against the protocol. Free-rider problems are well-known in economics (Buchanan, 1987) and manifest in blockchain networks whenever some nodes can benefit from the security provided by others without contributing their fair share of effort or resources. For example, in a decentralized public-records blockchain, a node might withhold information or avoid validating transactions to save costs, expecting others to do the work, if too many take this approach, the network's reliability degrades. Simulations have confirmed that the level of honest participation in such networks critically depends on the design of incentives, and that a fragile cooperative balance can collapse if incentives are not properly aligned (see section 4.2 article in the appendix). These considerations make it clear that blockchain protocol design is as much about mechanism design (an economics term for designing rules of a game to achieve desired outcomes) as it is about cryptography or distributed algorithms. The literature has begun to employ game theory as a tool to analyse these issues, modelling the strategic interactions among nodes and evaluating incentive

compatibility, i.e. whether each participant's best interest is to follow the rules under a given incentive scheme. So far, however, research combining game theory and blockchain consensus remains relatively scarce and has focused on a limited set of scenarios. This section contributes to this emerging field by providing new game-theoretic insights into both consensus mechanism design and DAO governance.

Most of the study summarised here is dedicated to voting-based consensus mechanisms in blockchain networks. Voting-based consensus refers to protocols (often used in permissioned or consortium blockchains) where validators vote on the validity of blocks or transactions, in contrast to pure proof-of-work mining. These protocols (e.g. Practical Byzantine Fault Tolerance and its variants) rely on coordinated voting and usually have different reward structures than proof-of-work or proof-of-stake. The study constructs a formal game-theoretic model to analyse a typical voting-based consensus, treating the agreement process as a game among validators. Two alternative reward schemes are compared (see section 4.1 article in the appendix for details) : for instance, one scheme might reward all validators equally for each round of consensus, while another might only reward those who voted with the majority (or who proposed the winning block). By comparing these incentive schemes, the analysis demonstrates how mechanism design can influence validators' willingness to adhere to protocol rules. Key findings indicate that certain reward structures lead to stronger incentive compatibility – that is, validators have a dominant strategy to behave honestly – whereas others can introduce misaligned incentives or vulnerabilities. For example, if rewards are too concentrated or winner-takes-all, validators might be tempted to form alliances or bribe others, undermining the protocol. On the other hand, if rewards are too evenly spread regardless of effort, free-riding behaviour might increase. The game-theoretic lens reveals trade-offs: a well-calibrated incentive scheme can discourage malicious behaviour (such as voting for invalid blocks or abstaining) by making honest participation the most beneficial strategy for each agent. This outcome is important for network integrity because when incentives align with protocol goals, the consensus algorithm can attain both security (resistance to attacks or cheating) and efficiency (timely agreement on the ledger) in a self-sustaining manner. The chapter illustrates this by deriving equilibrium conditions or agent payoff matrices under different schemes, showing under which conditions all rational nodes will follow the protocol. These results offer practical insights for blockchain designers: choosing the right incentive mechanism (reward and penalty structure) is as important as the cryptographic design of the consensus itself to ensure honest behaviour prevails.

Moreover, the analysis emphasizes long-term criteria such as economic viability and sustainability of consensus mechanisms. It argues that incentive design should also consider costs like energy consumption and required resources. For instance, while Proof-of-Work provides strong security incentives, it incurs high energy cost; thus, alternative consensus protocols (Proof-of-Stake, voting-based BFT, etc.) are evaluated not only on security, but on how they incentivize security with lower resource usage. The study highlights that an optimal mechanism must balance agent incentives with system efficiency: validators should be rewarded in a way that encourages participation and truth-telling, yet the protocol should avoid

wasteful expenditure of computational or energy resources (a point that ties into environmental sustainability goals). In summary, by viewing nodes as economic actors, the consensus-level analysis in this section shows that the robustness of a blockchain network is critically shaped by incentive compatibility. This game-theoretic approach yields a more precise understanding of participant behaviour than purely technical analyses, and it underscores the need to embed the rules of the game (the consensus algorithm's incentives) such that rational, self-interested behaviour by each node collectively leads to secure outcomes.

Beyond the consensus protocol, the chapter extends its scope to incentive mechanisms in blockchain-based organizations, especially DAOs. A DAO is essentially an organisational entity governed by smart contracts on a blockchain, without traditional hierarchical management, in which rules and decision-making processes are encoded transparently in code. They represent a novel approach to economic organization and governance, enabling members to coordinate and allocate resources in a decentralized manner. While technical research on DAOs has examined issues like smart contract vulnerabilities (e.g. the Reentrancy attack that led to The DAO collapse in 2016), there is a notable gap in understanding their economic and governance structures. This part of the study helps fill this gap by investigating how incentive mechanisms can support effective decentralized governance in DAOs, drawing parallels to the consensus incentive problems. The study applies the concept of incentive compatibility to the internal mechanisms of DAOs, for example, how tokens and voting rights are designed, how proposal/reward systems are set up, and how to prevent free-rider or collusion behaviour among members.

Through case studies and theoretical discussion (see section 2 of the article in the appendix for details), the study illustrates that DAO governance faces similar strategic challenges: participants may shirk responsibilities or collude if incentives permit, and the absence of a central authority means that the rules must be self-enforcing. One real-world illustration discussed is the infamous 2016 DAO attack, in which a hacker exploited a flaw in The DAO's smart contract to divert millions of dollars' worth of cryptocurrency. Analyses of this event (Mehar et al., 2019) have highlighted how misaligned incentives and insufficient checks facilitated the exploit. In general, the DAO context underscores that code-based governance is vulnerable unless economic incentives are correctly aligned to penalize bad actors and reward good actors. One of the main findings is that by implementing carefully designed token reward schemes and smart contract rules, DAOs can potentially overcome traditional organizational challenges related to coordination, accountability, and scalability. For instance, reward systems in a DAO (such as distributing tokens or dividends for contributions) need to be structured to encourage member engagement and honest participation in collective decisions. If members who contribute valuable work or accurate votes are rewarded, while free-riders or malicious actors receive no benefit (or are penalized), the DAO can self-regulate and achieve outcomes similar to a well-managed organization, but without centralized control. The analysis also notes that DAOs allow decentralizing authority in ways previously not possible: decision rights can be distributed among stakeholders, and smart contracts can automatically enforce majority decisions or predefined rules. This can enhance transparency and trust, as rules are

applied consistently by code. However, it also requires that the incentive design within those smart contracts is sound, or else the DAO could collapse (either through member apathy or exploitation). This section therefore bridges the micro-level incentive issues (how individuals behave in a system) with the macro-level governance of a decentralized organization, demonstrating that the same principles of incentive alignment apply at both levels.

Across the consensus and DAO analyses, the critical role of incentive mechanisms is reaffirmed. The analysis shows that well-designed incentives are pivotal not only for achieving secure and efficient consensus, but also for creating resilient, equitable, and sustainable decentralized organizations. In technical terms, aligning validators' incentives with protocol rules ensures network security and integrity because the participants are discouraged from attacks like double-spending or invalid voting because such actions are not in their economic interest. In organizational terms, aligning members' incentives in a DAO with the community's objectives ensures the DAO can function and grow because contributors are motivated to act in the common interest and governance can be maintained without central oversight. One important insight is that incentive compatibility links to the concept of embedded governance: blockchain consensus algorithms and DAO rules effectively serve as embedded institutional rules that guide agent behaviour (much like constitutions or policies do in traditional organizations). By viewing consensus protocols through the lens of institutional economics and agency theory, the chapter highlights how they mitigate coordination problems in decentralized networks (analogous to how good governance mitigates collective action problems in societies).

5.1 Institutional and policy implications of incentive compatibility in public-sector blockchains

Some implications can be drawn from the analysis of incentive compatibility described so far. First, the analysis underscores that incentive compatibility is not a narrow technical detail but a governance requirement. In public-sector settings, the relevant question is not only whether a protocol is secure under stylized assumptions about "honest" and "malicious" nodes, but whether the institutional rules embedded in a specific implementation make compliant validation a best response for the actors who actually operate the nodes. Validators face real costs (infrastructure, staff time, opportunity costs, reputational exposure) and may also face opportunities for private gains from deviation (delay, selective inclusion, collusion, or strategic non-participation). The institutional properties public authorities care about - integrity of records, auditability, due process, and credible non-manipulability - therefore depend on equilibrium incentives. This shifts the evaluation of blockchain initiatives from the question about the protocol work in principle to the protocol work in the incentive environment created by this governance configuration, with this validator set, and under these monitoring and sanctioning conditions.

Second, sustainable incentive alignment requires durable funding and credible sanctions, and this typically looks different in public-sector deployments than in open cryptocurrency networks. Many public-sector projects adopt permissioned or consortium architectures, frequently with restricted participation and limited (or absent) token-based rewards. In such contexts, validators often respond to budgetary allocations, contractual payments, service-level obligations, administrative accountability, and reputational or legal consequences. The implication of the micro-results is that these “off-chain” incentives must be treated as part of the effective incentive scheme. If validation imposes non-trivial marginal costs but remuneration is fixed, symbolic, or contingent on short political cycles, the equilibrium may drift toward minimal-effort behaviour: delayed validation, weak monitoring, reliance on a small subset of active nodes, and gradual degradation of the system’s reliability. Conversely, if rewards are tied mechanically to throughput (or to easily gameable metrics), validators may prioritize volume over scrutiny, undermining integrity, a particularly problematic outcome in public registries, procurement workflows, or audit trails where correctness and contestability matter more than raw transaction speed. A policy-relevant implication is that incentive design must be assessed over a multi-year horizon and coupled with stable governance and funding arrangements that preserve the integrity objective under routine operational stress and political turnover.

Third, validator incentives cannot be separated from governance design that allocates decision rights, update authority, and dispute-resolution procedures. Who is allowed to validate, who can modify rules, how conflicts are adjudicated, and how upgrades are approved jointly define the strategic environment. The analysis in this chapter cautions against governance arrangements that structurally embed conflicts of interest - such as configurations where the same actor submits transactions, validates them, and controls protocol rule changes - since these arrangements expand the payoff to deviation, collusion, or strategic opacity. A policy-relevant design principle is separation of duties: distributing validation, audit, and rule-update roles across actors with partially non-overlapping incentives (for example, operational agencies, oversight bodies, and independent auditors). Importantly, decentralization here should be interpreted institutionally rather than ideologically. For many public applications, the objective is not to eliminate state coordination, but to reduce unilateral discretion, make manipulation costly and detectable, and embed transparent accountability in routine operations.

Finally, these incentive considerations clarify why institutional setting is a binding constraint in public-sector blockchain adoption. Chapter 1 showed that barriers frequently include skills shortages, unclear governance responsibilities, and dependence on external providers. The micro-foundations developed here explain the mechanism: without internal capability to specify governance objectives, translate them into incentive-compatible rule systems, and monitor behaviour over time, public institutions may “adopt blockchain” in a technical sense while failing to secure the institutional properties that motivate adoption in the first place. Two actionable implications follow. (i) Blockchain initiatives should be treated as iterative governance projects with explicit monitoring of incentive outcomes (participation rates, validation delays, deviation indicators, dispute frequency), rather than as one-off IT

deployments. (ii) Procurement and governance literacy about incentive architecture - should be a core deliverable of public-private partnerships, not an externality. This is also consistent with the dissertation's broader view that blockchain's public value depends on the alignment between protocol-level incentives and the institutional context that steers and disciplines them.

5.1.1 Validator incentives, governance design, and public procurement

In public-sector implementations, procurement is not external to the incentive problem: it is one of its primary determinants. Procurement choices specify architecture (permissioned vs permissionless, single-agency vs consortium), the validator set (public agencies, audited third parties, external providers), compensation models (fixed fees, performance-based payments, transaction-based remuneration), and monitoring/sanctioning instruments (service-level agreements, penalties, termination rights, audit clauses). These contractual and organizational decisions define the payoffs faced by validators and therefore shape whether the deployed system is effectively incentive-compatible in its operational environment.

Consider a blockchain-based procurement ledger intended to strengthen traceability and constrain post-award manipulation. A configuration in which the implementation vendor operates most validating nodes may be efficient in the short run, but it concentrates validation authority in a party whose commercial incentives may diverge from the public interest in transparency, contestability, and long-run portability. By contrast, a consortium configuration that allocates validation and read-access rights across procurement authorities, auditing bodies, and independent oversight institutions can reduce unilateral control, but requires explicit governance rules for upgrades, dispute resolution, incident response, and accountability. In both cases, the incentive architecture is not only token-based: it includes contractual payoffs, reputational exposure, and legal responsibilities that can either reinforce or undermine the protocol's integrity objectives.

Two cautionary notes follow. First, procurement-driven decentralization can become symbolic if technical control remains effectively centralized through proprietary components, restricted auditability, or non-portable data models, conditions that increase lock-in risks and weaken institutional learning. Second, procurement must preserve administrative due process and contestability: automating parts of the workflow via smart contracts should not eliminate legally required discretion, appeal mechanisms, or human oversight. From an institutional-capability viewpoint, the key criterion is whether procurement and governance design strengthen the administration's ability to steer, audit, and update the system over time—rather than merely acquiring a technical artifact.

5.2 Micro-foundations and the conditional institutional claim

The results developed in this chapter strengthen a central inference of the dissertation: blockchain's governance properties cannot be inferred from cryptographic design alone,

because they are realized - or undermined - through strategic behaviour shaped by incentives. When validators are modelled as rational agents, protocol compliance is not a binary engineering assumption; it is an equilibrium outcome that depends on whether the incentive scheme makes honest validation individually rational under realistic costs, opportunities, and governance constraints. In this sense, incentive compatibility is the micro-level mechanism through which “trust by design” either emerges endogenously or fails in practice.

This micro-foundation also clarifies why the barriers documented in Chapter 1 are institutionally consequential. Skills shortages, governance ambiguity, reliance on external vendors, and regulatory uncertainty are not merely frictions that delay adoption; they constrain the public organization’s capacity to specify objectives, translate them into enforceable rule systems, and sustain those systems through monitoring and iteration. Where such capabilities are limited, blockchain projects risk remaining isolated pilots or devolving into externally governed infrastructures, thereby reproducing the familiar pattern of outsourced modernization without durable institutional learning.

From an institutional perspective, the key implication is that public-sector blockchain governance has two layers that must be aligned. The first is the protocol layer (consensus rules, validator incentives, and enforcement mechanisms). The second is the institutional layer (who operates validators, how responsibilities are allocated, how updates are approved, how disputes are resolved, and how accountability is maintained). The micro-results in this chapter imply that misalignment at either layer can defeat the integrity objective. A technically sophisticated protocol can still generate weak institutional outcomes if governance rights are concentrated, if monitoring is not credible, or if the payoff structure rewards minimal-effort participation. Conversely, even simple architectures can be institutionally robust when incentive-compatible designs are embedded in governance arrangements that preserve separation of duties, auditability, and enforceable accountability.

This leads directly to the dissertation’s conditional claim about “blockchain as institutional technology.” Its institutional character is implementation-dependent: it becomes institutionally meaningful only when public institutions possess (or build) the capability to design, evaluate, and govern incentive architectures over time. In practical terms, this capability includes procurement literacy about incentive schemes; technical competence sufficient to avoid governance-by-vendor; legal–institutional competence to preserve due process and contestability; and organizational competence to coordinate validation, oversight, and updating procedures across stakeholders.

Accordingly, the policy relevance of the chapter is not confined to selecting the “best” consensus protocol in the abstract. The deeper lesson is that sustainable public-sector deployments require incentive compatibility to be treated as a governance criterion, explicitly incorporated into institutional design choices, contracting arrangements, and monitoring frameworks. This micro-level insight complements the dissertation’s macro- and meso-level findings: if blockchain is to contribute to public-sector transformation, it must be embedded within governance arrangements that enable endogenous learning and preserve institutional agency, rather than functioning as a technically novel but externally controlled infrastructure.

Concluding remarks

This dissertation began from a historically grounded puzzle: despite recurrent waves of digital modernization in Western public administrations, the institutional outcomes of “technology-driven reform” have been uneven, often constrained by governance complexity, organizational inertia, and the difficulty of sustaining endogenous capability over time. Against this background, the dissertation asked whether blockchain should be understood not only as an information technology, but as a candidate institutional technology, one whose distinctive contribution lies in embedding governance rules, rights, and enforcement mechanisms into a shared digital infrastructure.

The five chapters jointly close this argument in a circular and cumulative way. Chapter 1 mapped the barrier landscape and showed that adoption obstacles in public organizations are rarely “just technical”, but they can be read diagnostically as capability constraints, interoperability and integration capacity, legal–regulatory alignment, organizational coordination, governance clarity, and the ability to learn rather than merely outsource. Chapter 2 then assessed, through a comparative diffusion exercise, whether blockchain behaves differently from a more pervasive digital technology (AI), finding patterns consistent with the view that institutional and governance conditions correlate strongly with observed uptake (while remaining cautious about causal interpretation). Chapters 3 and 4 explored the meso-level implications of blockchain as a coordination and governance infrastructure, proposing how decentralized rule systems can reshape organizational forms and how consensus mechanisms can be interpreted as institutional rule systems operating under agency constraints. Finally, Chapter 5 provided the micro-foundations: it formalized how incentive schemes shape equilibrium behaviour among validators, clarifying why “trust by design” is ultimately an outcome of incentive compatibility and governance design rather than a property of code alone.

Taken together, the findings of this dissertation provide a qualified answer to the central research question that is, whether - and under what conditions - blockchain may be conceptualized as an institutional technology in the public sector. These results support a conditional proposition that is central to the dissertation’s contribution: blockchain becomes institutionally meaningful in the public sector only when public organizations possess the capacity to design, steer, and progressively internalize the governance arrangements embedded in digital infrastructures.

In practice, this means that the institutional character of blockchain is implementation-dependent: it depends on whether public institutions can specify governance objectives, allocate decision rights responsibly, procure and supervise architectures without ceding de facto control, and iteratively monitor and revise the incentive and rule system as conditions evolve. Where such capability is absent, blockchain risks replicating familiar trajectories of

externally supplied modernization, producing pilots and technical artifacts without durable institutional learning or accountability gains.

From this standpoint, many of the barriers discussed throughout the dissertation — including interoperability constraints, regulatory ambiguity, skills shortages, and reliance on external vendors — should be interpreted not simply as obstacles slowing technological adoption, but as signals of limited public capability to design and govern incentive-compatible institutional infrastructures. Where such capability remains underdeveloped, even technically sophisticated blockchain systems may fail to generate durable improvements in trust, integrity, and accountability.

Drawing on the cumulative evidence developed across the macro, meso and micro-level analyses presented in the preceding chapters, three concise policy implications emerge from this conditional perspective. First, capacity building should be treated as a core objective of blockchain initiatives, not as a secondary benefit: public administrations need institutional, legal, and technical competence to steer governance-by-protocol over the full lifecycle (design, deployment, monitoring, upgrading, and incident response).

Second, procurement must be understood as governance: procurement choices implicitly define validator sets, payoffs, audit rights, upgrade authority, and dispute-resolution pathways, and therefore shape whether the deployed system's equilibrium behaviour aligns with public objectives. This dissertation shows that procurement decisions are not external to the incentive architecture of blockchain systems but are among its primary determinants. Choices concerning system architecture, validator configuration, compensation models, and contractual monitoring mechanisms directly shape the payoffs faced by network participants and therefore influence whether the resulting governance structure is effectively incentive-compatible. From an institutional perspective, procurement arrangements that concentrate technical control in external vendors may generate short-term efficiency but risk weakening transparency, contestability, and long-term administrative learning. Conversely, governance configurations that distribute validation authority across public institutions and independent oversight bodies can strengthen accountability, but require clearly specified rules for system upgrades, dispute resolution, and responsibility allocation. More broadly, the analysis suggests that public-sector blockchain governance operates simultaneously on two interdependent layers that must remain aligned over time. The first is the technical layer, defined by protocol rules, consensus mechanisms, and validator incentives. The second is the institutional layer, which concerns the allocation of decision rights, responsibility structures, monitoring arrangements, and accountability procedures within the administrative system. The findings of this dissertation indicate that misalignment between these layers can undermine the integrity and coordination objectives of blockchain initiatives. Even technically advanced architectures may generate weak institutional outcomes if governance rights are overly concentrated or if incentive structures do not sustain credible participation. Conversely, comparatively simple technical designs can support robust institutional performance when embedded in governance arrangements that preserve separation of duties, auditability, and enforceable accountability.

Third, incentive-compatible monitoring should be institutionalized: beyond ex ante design, governments should adopt monitoring frameworks that track participation, validation performance, deviation signals, and dispute frequencies, and that make adaptation of rules and incentives a legitimate, accountable administrative routine rather than an exceptional intervention.

The dissertation also has limitations. Most importantly, the cross-sectional nature of the empirical analysis constrains causal inference and does not capture how blockchain-related governance and capability evolve over time. In addition, the dissertation's scope is intentionally broad and multi-disciplinary, privileging integration across levels over exhaustive treatment of any single use case or jurisdiction.

These limitations motivate two targeted directions for future research. First, longitudinal and quasi-experimental designs - drawing on panel data, policy discontinuities, and institutional reforms - could test more directly how capability-building strategies and governance choices influence the trajectory and outcomes of blockchain adoption over time. Second, comparative institutional case studies focused on procurement, validator governance, and incentive monitoring could identify which organizational arrangements effectively preserve public agency while enabling credible multi-actor coordination, thereby operationalizing the dissertation's conditional claim in context-sensitive, policy-relevant terms.

References

- Abadi, J., & Brunnermeier, M. (2018). Blockchain Economics (w25407; Issue w25407, p. w25407). National Bureau of Economic Research. <https://doi.org/10.3386/w25407>
- Abeyratne, S., & Monfared, R. (2016). Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *International Journal of Research in Engineering and Technology*, 05.
- Abraham, I., Dolev, D., Gonen, R., & Halpern, J. (2006). Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. *Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing*, 53–62. <https://doi.org/10.1145/1146381.1146393>
- Akerlof, G. A. (1978). THE MARKET FOR “LEMONS”: QUALITY UNCERTAINTY AND THE MARKET MECHANISM*. In P. Diamond & M. Rothschild (Eds.), *Uncertainty in Economics* (pp. 235–251). Academic Press. <https://doi.org/10.1016/B978-0-12-214850-7.50022-X>
- Allen, D. W. E., Berg, C., Ilyushina, N., & Potts, J. (2023). Large Language Models Reduce Agency Costs (SSRN Scholarly Paper 4437679). Social Science Research Network. <https://doi.org/10.2139/ssrn.4437679>
- Allison. (2018). IBM and Maersk struggle to sign partners to shipping blockchain. CoinDesk. <https://www.coindesk.com/ibm-blockchain-maersk-shipping-struggling>
- Amoussou-Guenou, Y., Biais, B., Potop-Butucaru, M., & Tucci-Piergiovanni, S. (2023). Committee-Based Blockchains as Games between Opportunistic Players and Adversaries. *The Review of Financial Studies*, hhad051. <https://doi.org/10.1093/rfs/hhad051>
- Anderson, P., & Tushman, M. L. (1990). Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change. *Administrative Science Quarterly*, 35(4), 604. <https://doi.org/10.2307/2393511>
- Arrow, K. J. (1963, December 1). UNCERTAINTY AND THE WELFARE ECONOMICS OF MEDICAL CARE. | EBSCOhost. <https://openurl.ebsco.com/contentitem/gcd:8745671?sid=ebsco:plink:crawler&id=ebsco:gcd:8745671>
- Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the Semantic Web. *Journal of Web Semantics*, 5(2), 58–71. <https://doi.org/10.1016/j.websem.2007.03.002>
- Auer, R., Monnet, C., & Shin, H. S. (2021). Permissioned Distributed Ledgers and the Governance of Money. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3770075>
- Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., & Fridgen, G. (2023). Decentralised Finance’s timocratic governance: The distribution and exercise of tokenised voting rights. *Technology in Society*, 73, 102251. <https://doi.org/10.1016/j.techsoc.2023.102251>
- Bartlett, C. A., & Ghoshal, S. (1993). Beyond the M-Form: Toward a Managerial Theory of the Firm. *Strategic Management Journal*, 14, 23–46.

- Basterretxea, I., Cornforth, C., & Heras-Saizarbitoria, I. (2022). Corporate governance as a key aspect in the failure of worker cooperatives. *Economic and Industrial Democracy*, 43(1), 362–387. <https://doi.org/10.1177/0143831X19899474>
- Beck, R. (2018). Beyond Bitcoin: The Rise of Blockchain World. *Computer*, 51(2), 54–58. *Computer*. <https://doi.org/10.1109/MC.2018.1451660>
- Bekar, Carlaw, & Lipsey. (2018). General purpose technologies in theory, application and controversy: A review | *Journal of Evolutionary Economics*. <https://link.springer.com/article/10.1007/s00191-017-0546-0>
- Berg, C., Davidson, S., & Potts, J. (2017). Blockchains Industrialise Trust (SSRN Scholarly Paper 3074070). Social Science Research Network. <https://doi.org/10.2139/ssrn.3074070>
- Berg, C., Davidson, S., & Potts, J. (2018). Outsourcing Vertical Integration: Distributed Ledgers and the V-Form Organisation (SSRN Scholarly Paper 3300506). Social Science Research Network. <https://doi.org/10.2139/ssrn.3300506>
- Berg, C., Davidson, S., & Potts, J. (2019). *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*. Edward Elgar Publishing.
- Berg, C., Davidson, S., & Potts, J. (2020). Trustless Architecture and the V-Form Organisation (SSRN Scholarly Paper 3612419). Social Science Research Network. <https://doi.org/10.2139/ssrn.3612419>
- Bleeckcer. (1994). The virtual organization. <https://www.proquest.com/openview/39237fa7874b2cedc1375dd78d1b66bb/1.pdf?pq-origsite=gscholar&cbl=47758>
- Braverman, H. (1998). *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*. NYU Press.
- Cachin, C., & Vukolic, M. (2017). Blockchain Consensus Protocols in the Wild (Keynote Talk) [Application/pdf]. 16 pages. <https://doi.org/10.4230/LIPICS.DISC.2017.1>
- Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, 20(4), Article 4. <https://doi.org/10.1145/571637.571640>
- Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM*, 63(7), Article 7. <https://doi.org/10.1145/3359552>
- Chandler, A. D. (1977). *The Visible Hand: The Managerial Revolution in American Business*. Harvard University Press.
- Chandler. (1966). *Strategy and Structure: Chapters in the History of the Industrial Enterprise*. Doubleday.
- Chen, L., Cong, L. W., & Xiao, Y. (2020). A Brief Introduction to Blockchain Economics. In K. R. Balachandran, *Information for Efficient Decision Making* (pp. 1–40). WORLD SCIENTIFIC. https://doi.org/10.1142/9789811220470_0001
- Chi, T., Nystrom, P. C., & Kircher, P. (2003). *Knowledge, Scope, and Internal Organization of the Multinational Corporation*.
- Coase, R. H. (1937). The Nature of the Firm. *Economica*, 4(16), 386–405. <https://doi.org/10.2307/2626876>

- Constant, E. W. I. (1973). A Model for Technological Change Applied to the Turbojet Revolution. *Technology and Culture*, 14(4), 553–572.
- Davidow, & Malone. (1992). *The Virtual Corporation: Structuring and Revitalizing The Corporation For The 21 st Century*.
- Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4), 639–658. <https://doi.org/10.1017/S1744137417000200>
- De Angelis, Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. *CEUR Workshop Proceedings*, 2058. https://iris.uniroma1.it/bitstream/11573/1337256/1/DeAngelis_PBFT_2018.pdf
- Dib, A., Brousmiche, K., Durand, A., Thea, E., & Hamida, E. D. (2018). Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, 51–64.
- Dopfer, K., Foster, J., & Potts, J. (2005). Micro-Meso-Macro (SSRN Scholarly Paper 721599). Social Science Research Network. <https://papers.ssrn.com/abstract=721599>
- Dosi, G. (1982). Technological paradigms and technological trajectories: A suggested interpretation of the determinants and directions of technical change. *Research Policy*, 11(3), 147–162. [https://doi.org/10.1016/0048-7333\(82\)90016-6](https://doi.org/10.1016/0048-7333(82)90016-6)
- Edwards, R. (1982). Contested Terrain: The Transformation of the Workplace in the Twentieth Century. *Science and Society*, 46(2), 237–240.
- Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *The Academy of Management Review*, 14(1), 57–74. <https://doi.org/10.2307/258191>
- Fligstein. (2000). The Spread of the Multidivisional Form Among Large Firms, 1919-1979. <https://www.jstor.org/stable/2095547>
- Franke. (2001). The concept of virtual web organizations and its implications on changing market conditions. *Electronic Journal of Organizational Virtualness*.
- Frolov, D. (2021). Blockchain and institutional complexity: An extended institutional approach. *Journal of Institutional Economics*, 17(1), 21–36. <https://doi.org/10.1017/S1744137420000272>
- Goldman, S. L., Nagel, R. N., & Preiss, K. (1995). *Agile Competitors and Virtual Organizations: Strategies for Enriching the Customer*.
- Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Structural Biotechnology Journal*, 16, 224–230. <https://doi.org/10.1016/j.csbj.2018.06.003>
- Groce, A., Katz, J., Thiruvengadam, A., & Zikas, V. (2012). Byzantine Agreement with a Rational Adversary. In A. Czumaj, K. Mehlhorn, A. Pitts, & R. Wattenhofer (Eds.), *Automata, Languages, and Programming* (Vol. 7392, pp. 561–572). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-31585-5_50
- Grover, P., Kar, A. K., & Janssen, M. (2019). Diffusion of blockchain technology: Insights from academic literature and social media analytics. *Journal of Enterprise Information Management*, 32(5), Article 5. <https://doi.org/10.1108/JEIM-06-2018-0132>

Hadfield-Menell, D. J. (2021). The Principal–Agent Alignment Problem in Artificial Intelligence.

Halpern, J., & Teague, V. (2004). Rational secret sharing and multiparty computation: Extended abstract. *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, 623–632. <https://doi.org/10.1145/1007352.1007447>

Hart, O. D. (1986). *The theory of contracts*.

Hasselgren, A., Krlevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, 134, 104040. <https://doi.org/10.1016/j.ijmedinf.2019.104040>

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54, 102136. <https://doi.org/10.1016/j.ijinfomgt.2020.102136>

Hill, C. W. L., & Hoskisson, R. E. (1987). Strategy and Structure in the Multiproduct Firm. *The Academy of Management Review*, 12(2), 331–341. <https://doi.org/10.2307/258539>

Ibrahimi, 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. <https://doi.org/10.1016/j.bcra.2023.100186>

Jabbar, A., & Dani, S. (2020). Investigating the link between transaction and computational costs in a blockchain environment. *International Journal of Production Research*, 58(11), Article 11. <https://doi.org/10.1080/00207543.2020.1754487>

Kaal, W. A. (2020). Blockchain-Based Corporate Governance. *Stanford Journal of Blockchain Law & Policy*, 4, 3.

Kamal, R., Hemdan, E. E.-D., & El-Fishway, N. (2023). Care4U: Integrated healthcare systems based on blockchain. *Blockchain: Research and Applications*, 100151. <https://doi.org/10.1016/j.bcra.2023.100151>

Kane, E. (2017). Is Blockchain a General Purpose Technology? (SSRN Scholarly Paper 2932585). Social Science Research Network. <https://doi.org/10.2139/ssrn.2932585>

Khalil, O., & Wang, S. (2002). Information technology enabled meta-management for virtual organizations. *International Journal of Production Economics*, 75(1), 127–134. [https://doi.org/10.1016/S0925-5273\(01\)00186-4](https://doi.org/10.1016/S0925-5273(01)00186-4)

Kogut & Parkinson. (1998). *Adoption of the Multidivisional Structure: Analyzing History from the Start | Industrial and Corporate Change | Oxford Academic*. <https://academic.oup.com/icc/article-abstract/7/2/249/678169>

Kraakman, R., Armour, J., Davies, P., Enriques, L., Hansmann, H., Hertig, G., Hopt, K., Kanda, H., Pargendler, M., Ringe, W.-G., & Rock, E. (2017). *The Anatomy of Corporate Law: A Comparative and Functional Approach*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780198739630.001.0001>

Kuhn, T. S. (1962). *The structure of scientific revolutions*. University of Chicago press.

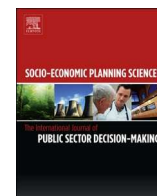
Landes. (1969). *The unbound Prometheus: Technological change and industrial development in Western Europe from 1750 to the present*.

- Li, X., Liu, Q., Wu, S., Cao, Z., & Bai, Q. (2023). Game theory based compatible incentive mechanism design for non-cryptocurrency blockchain systems. *Journal of Industrial Information Integration*, 31, 100426. <https://doi.org/10.1016/j.jii.2022.100426>
- Lukas, C., & Schöndube, J. R. (2012). Trust and adaptive learning in implicit contracts. *Review of Managerial Science*, 6(1), 1–32. <https://doi.org/10.1007/s11846-010-0045-2>
- Mannan, M. (2023). The Promise and Perils of Corporate Governance-by-Design in Blockchain-Based Collectives: The Case of dOrg. <https://bristoluniversitypressdigital.com/edcollchap/book/9781529226430/ch005.xml>
- Marglin, S. A. (1974). What Do Bosses Do?. The Origins and Functions of Hierarchy in Capitalist Production. *Review of Radical Political Economics*, 6(2), 60–112. <https://doi.org/10.1177/048661347400600206>
- Martinelli, A. (2012). An emerging paradigm or just another trajectory? Understanding the nature of technological changes using engineering heuristics in the telecommunications switching industry. *Research Policy*, 41(2), 414–429. <https://doi.org/10.1016/j.respol.2011.10.012>
- Michaud, M., & Audebrand, L. K. (2022). One governance theory to rule them all? The case for a paradoxical approach to co-operative governance. *Journal of Co-Operative Organization and Management*, 10(1), 100151. <https://doi.org/10.1016/j.jcom.2021.100151>
- Mokyr, J. (Ed.). (2005). *The gifts of Athena: Historical origins of the knowledge economy*. Princeton University Press.
- Moura, L. M. F. de, Brauner, D. F., & Janissek-Muniz, R. (2020). Blockchain and a Technological Perspective for Public Administration: A Systematic Review. *Revista de Administração Contemporânea*, 24, 259–274. <https://doi.org/10.1590/1982-7849rac2020190171>
- Murano, A., Bruno, B., & Vespri, V. (2024). Incentive Compatibility In Consensus Protocols And DAOs: A Game-Theoretic Approach.
- Murano, A., Bruno, B., & Vespri, V. (2025). Blockchain Barriers in Public Organizations: A Systematic Literature Review. *Socio-Economic Planning Sciences*, 102364. <https://doi.org/10.1016/j.seps.2025.102364>
- Nakamoto, S. (2008). *A Peer-to-Peer Electronic Cash System*.
- Nelson, R. R., & Winter, S. G. (1985). *An Evolutionary Theory of Economic Change*. Harvard University Press.
- Nguyen, G.-T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information Processing Systems*, 14(1), Article 1. <https://doi.org/10.3745/JIPS.01.0024>
- North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge University Press.
- Ohno, T. (1988). *Toyota Production System: Beyond Large-Scale Production*. CRC Press.
- Okada, H., Yamasaki, S., & Bracamonte, V. (2017). Proposed classification of blockchains based on authority and incentive dimensions. 2017 19th International Conference on

- Advanced Communication Technology (ICACT), 593–597.
<https://doi.org/10.23919/ICACT.2017.7890159>
- Oyinloye, D. P., Teh, J. S., Jamil, N., & Alawida, M. (2021). Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry*, 13(8), Article 8.
<https://doi.org/10.3390/sym13081363>
- Pargendler, M. (2016). The Corporate Governance Obsession. *Journal of Corporation Law*, 42, 359.
- Pollard, S. (1968). *The genesis of modern management: A study of the industrial revolution in great britain*. Penguin Books. <https://cir.nii.ac.jp/crid/1130282270583752192>
- Qian, Y., Roland, G., & Xu, C.-G. (2003, June). Coordinating tasks in M-form and U-form organisations [Monograph]. Suntory and Toyota International Centres for Economics and Related Disciplines. <http://sticerd.lse.ac.uk/>
- Riemer, K., & Klein, S. (2008). Is the V-form the Next Generation Organisation? An Analysis of Challenges, Pitfalls and Remedies of ICT-enabled Virtual Organisations Based on Social Capital Theory. *Journal of Information Technology*, 23(3), 147–162.
<https://doi.org/10.1057/palgrave.jit.2000120>
- Rosenberg, N. (1974). Karl Marx on the Economic Role of Science. *Journal of Political Economy*, 82(4), 713–728.
- Ross, S. A. (1973). The Economic Theory of Agency: The Principal's Problem. *The American Economic Review*, 63(2), 134–139.
- Rothschild, M., & Stiglitz, J. (1976). Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. *The Quarterly Journal of Economics*, 90(4), 629.
<https://doi.org/10.2307/1885326>
- Rüttimann, B. G., & Stöckli, M. T. (2016). Going beyond Triviality: The Toyota Production System—Lean Manufacturing beyond Muda and Kaizen. *Journal of Service Science and Management*, 9(2), Article 2. <https://doi.org/10.4236/jssm.2016.92018>
- Saabeel, Verduijn, Hagdorn, & Kumar. (2002). A model of virtual organization: A structure and process perspective.
- Shah, N. (2024). Hybrid-DAOs: Enhancing Governance, Scalability, and Compliance in Decentralized Systems (arXiv:2410.21593). arXiv.
<https://doi.org/10.48550/arXiv.2410.21593>
- Spear, R. (2004). Governance in Democratic Member-Based Organisations. *Annals of Public and Cooperative Economics*, 75(1), 33–60. <https://doi.org/10.1111/j.1467-8292.2004.00242.x>
- Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, 355–374.
- Sukhwani, H., Martinez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017). Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric). 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 253–255.
<https://doi.org/10.1109/SRDS.2017.36>
- Swanson, T. (2015). Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems.
- Taylor, F. W. (1911). *The principles of scientific management*. Noton & Company.

- 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.
- Tuma, A. (1998). Configuration and coordination of virtual production networks. *International Journal of Production Economics*, 56–57, 641–648. [https://doi.org/10.1016/S0925-5273\(97\)00146-1](https://doi.org/10.1016/S0925-5273(97)00146-1)
- Venkatraman & Henderson. (1998). Real Strategies for Virtual Organizing. https://www.proquest.com/openview/3fabd6a5bcfcd15d013e871ecd411f27/1?pq-origsite=gscholar&cbl=26142&casa_token=1XWC5ms00mcAAAAA:4wbLudmQnhSiJJFEYvtoThyrmuuSQ51o4kbvhp9rJMtvtwkvX_CkHEI5M_-irFQ3SST0Q
- Vincenti, W. G. (1990). What engineers know and how they know it (Vol. 141). Baltimore: Johns Hopkins University Press. <https://cache.fluxo.info/data/43/fd/43fd869e20dd2bd5981913825ac4b9bbacaec441/screenshot.pdf>
- Vincenti, W. G. (1994). The Retractable Airplane Landing Gear and the Northrop ‘Anomaly’: Variation-Selection and the Shaping of Technology. *Technology and Culture*, 35(1), 1–33. <https://doi.org/10.2307/3106747>
- Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., & Wang, F.-Y. (2019). Decentralized Autonomous Organizations: Concept, Model, and Applications. *IEEE Transactions on Computational Social Systems*, 6(5), 870–878. <https://doi.org/10.1109/TCSS.2019.2938190>
- Williamson, O. (1985). The Economic Institutions of Capitalism. Firms, Markets, Relational Contracting. https://link.springer.com/chapter/10.1007/978-3-8349-9320-5_6
- Williamson, O. E. (1963). Managerial Discretion and Business Behavior. *The American Economic Review*, 53(5), 1032–1057.
- Williamson, O. E. (1975). Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization (SSRN Scholarly Paper 1496220). Social Science Research Network. <https://papers.ssrn.com/abstract=1496220>
- Williamson, O. E. (1983). Organization Form, Residual Claimants, and Corporate Control. *The Journal of Law & Economics*, 26(2), 351–366.
- Williamson, O. E. (1996). The Mechanisms of Governance. Oxford University Press.
- Womack, J. P., Jones, D. T., & Roos, D. (2007). The Machine That Changed the World: The Story of Lean Production-- Toyota’s Secret Weapon in the Global Car Wars That Is Now Revolutionizing World Industry. Simon and Schuster.

ARTICLES



Review

Blockchain barriers in public organizations: A systematic literature review

Angelo Murano^{*}, Bruna Bruno, Vincenzo Vespri

University of Salerno, Italy



ARTICLE INFO

Keywords:

blockchain
Distributed ledger
public sector
Interoperability
Governance
Technology adoption
digital transformation

ABSTRACT

Blockchain technology has garnered attention for its potential to revolutionize public sector services by enhancing transparency, efficiency, and trust. However, adoption remains hindered by critical organizational and technical barriers, which are underexplored in current literature, particularly from an economic-organizational perspective. This paper systematically reviews recent studies to identify sector-specific challenges, including interoperability issues and a shortage of technical expertise. By addressing these barriers, the findings propose tailored strategies to facilitate effective implementation, offering practical insights for public sector stakeholders and laying a robust foundation for future research.

1. Introduction

Blockchain technology is recognized as a General Purpose Technology (GPT) [1], with applications extending beyond cryptocurrencies. Interest in its non-cryptocurrency use has significantly grown in recent years.

Blockchain, the leading distributed ledger technology, consists of linked data blocks forming a continuous chain, managed through a decentralized peer-to-peer network. As noted by Yaga et al. [2], transactions in blockchain systems are cryptographically secured, transparent, and immutable, and are usually processed without a central authority. Blockchain can significantly enhance public sector services by improving security, accountability, transparency, and efficiency. Such benefits, however, are often counter-balanced by organisational and institutional barriers that remain under-researched. Public records management and healthcare are key promising application areas [3]. It can streamline registration processes, increase reliability, eliminate paper documents [4], and give citizens greater control and traceability over their healthcare data.

Recent literature highlights potential blockchain benefits and challenges in the public sector, emphasizing rapid technological evolution [5]. However, empirical studies based on concrete cases are scarce [6], and analyses on integration barriers are limited [7].

Policy discussions on blockchain emphasize economic potential and seek best practices, addressing governance, legal implications, interoperability, security, and privacy. Nonetheless, practical deployment remains limited compared to other technologies.

Existing reviews often neglect an economic-organizational perspective and rarely differentiate public from private sector applications, highlighting the originality and relevance of this study.

This paper systematically reviews blockchain applications in the public sector, conceptualizing innovation as "a process by which new ideas, objects, and practices are generated, evolved, or transformed, and which are novel to the adopting entity" [8], without prescriptive biases. Furthermore, results from literature review is compared with data available on 270 blockchain applications in the public sector.

The 'Preferred Reporting Items for Systematic Reviews and Meta-Analyses' (PRISMA) approach [9] was applied to identify relevant studies, followed by a text mining analysis to extract key themes. The findings highlight significant opportunities and context-specific challenges, particularly in healthcare, education, data management, public finance, and e-voting. The most recurrent challenges include issues of interoperability and a lack of technical expertise, emphasizing the necessity for tailored integration strategies.

Practical implications emphasize the importance of investment in training, infrastructure, and clear regulatory frameworks for privacy, data protection, and stakeholder accountability. Public trust through transparency and education is also crucial.

The originality of this study lies in addressing economic-organizational barriers specific to the public sector, filling a gap identified in previous literature. This paper consolidates fragmented research and provides an evidence-based overview, contributing a foundation for future research.

The structure of the paper is as follows: the Introduction outlines

^{*} Corresponding author.

E-mail addresses: amurano@unisa.it (A. Murano), brbruna@unisa.it (B. Bruno), vincenzo.vespri@unifi.it (V. Vespri).

blockchain's potential, identifies the research gap and objectives. The Related Work section reviews blockchain adoption literature and introduces research questions. In Section 3 the methodology is described, whereas Section 4 presents and discusses the main results. In Section 5 results from literature review are compared with data from European case studies. Finally, the Conclusions summarize contributions and suggest future research directions.

2. Related work and research questions

Despite the large number of publications on blockchain, most reviews still gravitate toward fintech and digital-currency themes [10,11], leaving non-crypto applications under-explored. The interdisciplinary nature of blockchain, spanning computer science, economics, management, and organizational studies, has led to a fragmented literature: technical analyses often ignore economic and organizational incentives, while managerial studies overlook key technical constraints such as interoperability and scalability. Yet effective public-sector adoption requires integrating these perspectives to address both socio-technical governance and organizational design. While economics takes a distinctive approach to problem-solving and decision-making, based on agents' behaviours and their interactions, computer science primarily focuses on system design, algorithm optimization, and information management. An interdisciplinary approach is needed to address critical technical issues, such as interoperability and scalability, without losing sight of the economic-organizational dynamics, such as resistance to change and cultural barriers. As a continuously expanding technology, updating the state of the art is important, possibly on an annual basis [5].

In the existing literature, not all reviews adopt an economic-organizational perspective. To fully investigate how blockchain may affect public or private organizations and their organizational structures, it is important to highlight major challenges the adoption of blockchain implies. Some authors have noted the lack of studies investigating and examining the barriers to blockchain integration in the public sector, proposing to fill this gap [7]. In the literature on innovation, these are frequently referred to as innovation barriers [12,13]. Recognizing and comprehending these barriers is considered a key factor for the successful management of the adoption process [14,15].

A specific limit to existing reviews lies in the lack of attention on the public sector. Although several studies have conceptually or empirically analysed the barriers to blockchain integration at the organizational level [16–19], seeking to understand why, despite its benefits, organizations struggle to implement this technology [20], they have not focused specifically on the public sector. While there are other reviews in the literature focused on this area [3,5], many focus on specific domains-such as e-government, smart contracts or digital infrastructure. The specificity of the public sector lies in the different nature of the goals pursued. In the private sector, organizational strategies frequently emphasize economic efficiency and control over resources, whereas in the public sector objectives involve not only economic dimensions but also social, political, and institutional goals. In this context, decisions may generate both direct resource impacts and broader social or institutional consequences (Meccheri, 2003).

A few notable contributions illustrate both progress and gaps. Moura, Brauner, & Janissek-Muniz [21] highlight blockchain's potential for enhancing information security, data openness, and citizen participation, emphasizing transparency and the use of smart contracts in public procurement. Rodríguez Bolívar & Scholl [22] map the nascent body of knowledge in blockchain applications for Digital Government. They indicate the current literature's bias toward fintech and identify a significant research gap regarding public-sector-specific studies. Their analysis advocates further research on legal frameworks, governance models, trust, transparency, democratic impacts, and public-sector reform enabled by blockchain. Even the most recent academic reviews, which testify to a growing interest in the economic sphere towards the

topic [23,24], do not specifically address the barriers to the blockchain integration in the public sector.

To address gaps in the existing literature, this review pursues an explicitly interdisciplinary and economic-organizational perspective. It investigates two research questions.

- **RQ1:** How is blockchain technology integrated into the public sector?
- **RQ2:** What organizational and technical challenges does the public sector face when integrating blockchain technology?

The RQ2 can be considered as sub-level question within RQ1. Accordingly, a two-step analysis is conducted: (i) database search and study selection, and (ii) data extraction and thematic analysis of both questions. For RQ1, themes are derived from the diverse areas of public administration potentially affected, such as healthcare, education, e-voting, and public finance. The thematic aspect of RQ2 lies in the bijective relationship between benefits and obstacles on the one side, and sector of analysis on the other side. This issue is addressed through a text mining technique. More detailed discussion is in the following methodological section.

Methodologically, the review analyses academic literature as the primary unit of evidence, contextualizing institutional settings and project examples reported in the selected studies. Barriers are synthesized as conceptual insights rather than as project-specific observations, enabling a systematic understanding of the factors that shape blockchain adoption in the public sector. It is also important to note that the relationship between challenges or benefits and the sectors involved is not strictly sector-specific or one-to-one. Some opportunities and obstacles may span across both public and private domains. Furthermore, the barriers are synthesized here as conceptual categories emerging from scholarly research, rather than as empirical observations from individual projects.

3. Methodology

To investigate the integration challenges of blockchain technology within the public sector, a Systematic Literature Review (SLR) as a standalone and independent study is conducted. This work helps to establish a comprehensive understanding of a research domain by collecting and synthesizing findings from multiple empirical studies [25, 26]. This approach uncovers the state of knowledge in fields characterized by diverse lines of inquiry and interdisciplinarity, identifying critical areas where further research is needed [27,28]. To minimize bias and reach reliable conclusions, a transparent, reproducible, and step-by-step methodology is adopted [26]. The method unfolds in two stages: (i) database search and study selection; (ii) data extraction and analysis.

3.1. Database search and studies selection

To identify eligible articles, we searched Scopus and Google Scholar to capture the field's interdisciplinarity (computer science, economics, management, organizational studies). The search was made with filters concerning document types and publication years. The initial literature search was conducted in February 2024 and was subsequently updated through a top-up search in July 2024, specifically to capture early-access and recently indexed publications. The review covers literature published from January 2020 through early 2024, up to the point when the SLR process was initiated. While this two-step approach mitigates potential bias due to time-lagged indexing, it is still possible that some papers published in late 2024 were not yet available in the databases at the time of the search. Given this pace of change, a five-year review window seems appropriate and ensures coverage of the post 'hype-cycle' policy landscape.

Following prior studies, keywords were selected to identify relevant

academic publications [29]. Queries combined terms for the public sector/administration, blockchain, and integration barriers/challenges (e.g., “public sector”, “government”, “public administration”, “blockchain”, “challenges”, “barriers”, “organizational”, “technical”). For the purposes of this research, the definition of the public sector adopted is from the OECD (2008). Specifically, the concept of “*public sector*” comprises all government-owned and government-operated entities and services, with the primary functions of providing public goods and services, markets regulations, and implementing public policies [30]. Examples include government ministries, public schools, public hospitals, police departments, and public transportation services [31].

Conversely, the idea of “*public administration*” involves the implementation of government policy and the management of public programs [32]. Functions of public administration include policy formulation, budgeting, human resource management, and the administration of public programs [33]. Examples include drafting regulations, managing public funds, overseeing government projects, and delivering public services [34]. Therefore, the distinction between the concepts of “*public sector*” and “*public administration*” entails that the public sector refers to the “*what*,” while public administration refers to the “*how*,” involving the execution government policies [31,35]. The query refinement process used to select articles is detailed in Table A1 of the Appendix.

The ‘Preferred Reporting Items for Systematic Reviews and Meta-Analyses’ (PRISMA) approach [9] was employed to identify eligible studies. The articles eligibility followed four phases: definition of inclusion and exclusion criteria, title and abstract analysis, full-text assessment, and cross-referencing check.

Inclusion and exclusion criteria were applied to ensure high-quality and relevant articles. Articles published in the last five years, written in English, peer-reviewed, and focusing on blockchain integration challenges in the public sector were included. While grey literature - such as reports, dissertations, and working papers - can offer valuable contextual insights, this review focused exclusively on peer-reviewed academic publications and grey sources were not included in the core analysis. Nonetheless, select insights from non-peer-reviewed documents will be referenced in the Discussion section, where appropriate. Inclusion and exclusion criteria are detailed in Table 1.

Using the databases Scopus and Google Scholar, a check for potential duplicates was performed, and none were identified. At the end of this phase, 258 articles were identified. The description of the methodological process used in the review is summarized in the flowchart in Fig. 1.

In the subset of articles matching the inclusion and exclusion criteria, a title and abstract analysis is performed. The authors independently read titles and abstracts to determine whether each publication met the inclusion criteria [29,51]. The titles and abstracts evaluation has led to the exclusion of 174 articles that did not satisfy the criteria. The full texts of the remaining 84 articles were then scrutinized through a full-text assessment, resulting in the exclusion of an additional 47 articles. Ultimately, 37 articles were deemed suitable for the review. Finally, a cross-referencing check was conducted. The references of the selected

Table 1
Inclusion and exclusion criteria.

Criteria	Inclusion	Exclusion
Publication Date	Articles published within the last 5 years	Articles published before the last 5 years
Research Focus	Focus on blockchain integration challenges in the public sector	Not addressing the integration challenges or not focused on the public sector
Language	English	Non-English languages
Document Type	Peer-reviewed academic articles	Editorials, opinion pieces, review papers, grey literature
Relevance	Directly addresses research questions	Does not contribute to research questions

Table 2

Use cases of blockchain in the public sector (RQ1).

Application Domain	Use Case Description	References
<i>Healthcare</i>	Management of medical records, interoperability, and privacy.	R. Zhang et al. [36]; Dhingra et al. [37]; Lu et al. [38]; Mustafa et al. [39]; Verma and Sheel [40]; Bustamante et al. [41]
<i>Education</i>	Verification of academic credentials and digital identity.	Tan et al. [42]; Dash et al. [43]; Haneem et al. [44]
<i>Data Management</i>	Reliability, transparency, and security for sensitive data.	Lu et al. [38]; Mustafa et al. [39]; R. Zhang et al. [36]; Clavin et al. [45]; Du et al. [46]; Anyanwu et al. [47]
<i>Public Finance</i>	Crowdfunding, fund management, and financial auditing.	Radynskyy et al. [48]; Hung [49]; Prux et al. [50]
<i>E-voting</i>	Security and transparency in electoral processes.	Clarke et al. (2023); Verma and Sheel [40]

articles are examined, but no additional studies meeting the criteria were found. The year distribution of the selected publications is shown in Fig. A3, whereas the distribution of publications by country is in Fig. A4.

Article-level country attribution was adopted as a comparable unit of analysis. The observed geographical distribution also opens the possibility that contextual factors - such as institutional capacity or trust in government - may influence adoption dynamics. This interpretation is further explored in the Discussion section, where supporting evidence from the literature is presented.

3.2. Data extraction and analysis

We applied thematic analysis (Clarke et al., 2023), combining manual coding with a Python-based text-mining module to enhance transparency and replicability. The process comprised.

1. Familiarization.
2. Label Creation.
3. Defining and Naming Themes.

We also conducted a structured qualitative appraisal of the 37 studies included in the review. Each study was categorized by methodological type (e.g., literature review, survey, case study, etc.), and an evaluation of its main strengths and limitations was provided. This qualitative assessment, aimed to complement the data-driven analysis, is synthesized in Appendix (see Table A4), providing an overview of the study types, their distribution, and the main qualitative observations.

In phase 1 of data extraction and analysis, each of 37 selected article was read to fully understand its content and context. The familiarization phase is the base for the Label Creation phase, which is needed to define the themes. Accordingly, the main keywords to be investigated through text mining are identified. In response to RQ1, it emerges that multiple areas involved in public sector activities may potentially be affected by blockchain adoption. In response to RQ2, labels were identified to highlight the main challenges and obstacles to blockchain adoption in the public sector.

In the third phase of the process, a Python-based text mining technique was integrated to extract from the full texts and their frequencies. For RQ1, the co-occurrence of key terms informed the classification of articles into thematic clusters, summarized in Table A2. For RQ2, Table A3 outlines the main organizational challenges in blockchain adoption based on their frequency and recurrence.

To the best of our knowledge, no prior studies have employed this methodology for examining organizational and technical barriers to blockchain adoption in the public sector. This allowed to identify

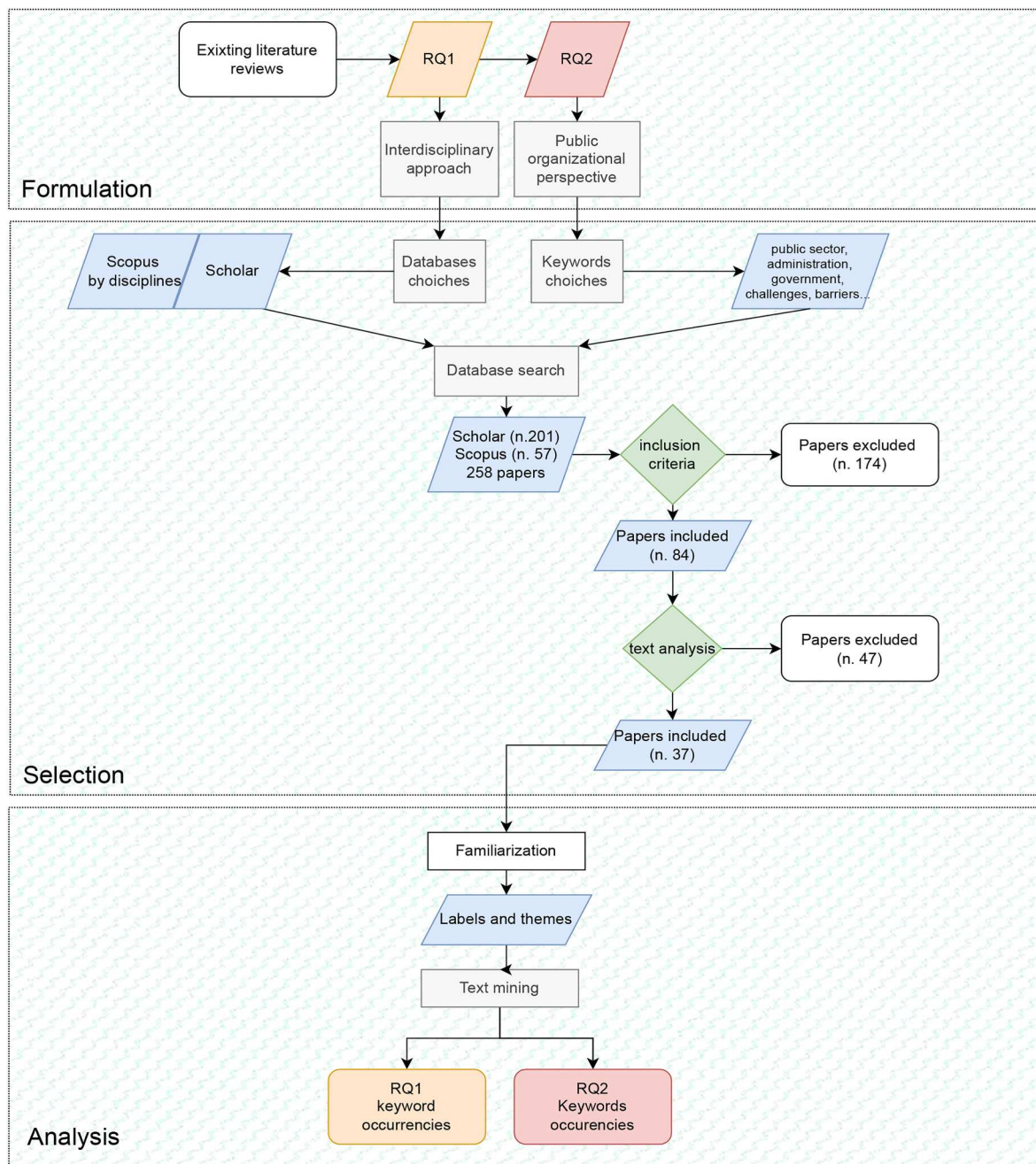


Fig. 1. Flowchart of SLR.

emergent themes and quantify their frequency, offering a robust foundation for addressing RQ2. Moreover, the insights derived from the coding process provided additional validation for the findings related to RQ1, which had been addressed using Boolean operators.

4. Results of the SLR

In this section, the main findings from the review are synthesized and discussed, addressing the two research questions.

RQ1: How is blockchain technology integrated into the public sector?

RQ2: What organizational and technical challenges does the public sector face when integrating blockchain technology?

Our review indicates a recent and increasing focus on the potential applications and research evolution of blockchain within the public sector, but a relatively small number of articles and journals with multiple contributions on this topic was found. The publication pattern and limited body of literature suggest that this area is still in its developmental stage [25].

4.1. Blockchain integration in the public sector (RQ1)

Addressing RQ1, the adoption of blockchain in the public sector reveals both substantial opportunities and significant challenges. The most frequent application areas identified include healthcare, education, data management, public finance, and e-voting. The distribution of article citations relevant to the domain analysed in relation to the first research question is presented in Table A5 of the Appendix.

4.1.1. Healthcare

Blockchain offers attributes that could revolutionize healthcare systems, particularly in patient data management, improving interoperability and protecting privacy. It is recognized as a reliable solution for storing and managing electronic health records (EHRs). Blockchain could be used to establish a chronological record of patient data, allowing both patients and doctors to efficiently review and analyse medical information [36].

In terms of interoperability, blockchain addresses current challenges related to ineffective communication between healthcare institutions. Storing health records on a blockchain could create a unified system accessible to authorized stakeholders. A study examining a distributed electronic health records ecosystem using blockchain technology found improvements in processing capacity, information sharing, and organizational flexibility [37].

Privacy is a critical concern when handling sensitive health data, particularly in the context of digital infrastructures. While blockchain is often promoted as a secure and transparent technology, its core strength lies in ensuring data integrity and traceability, rather than confidentiality. Some studies argue that blockchain may offer improved privacy protections compared to traditional health data storage systems [38], particularly when combined with encryption, identity management, and access control mechanisms [39]. However, these enhancements rely on off-chain architectures and complementary systems, and do not stem from the native properties of blockchain itself.

One often-cited example of blockchain application in healthcare is Estonia's e-Health Record system, which does not store medical records on-chain but uses blockchain to secure access logs and ensure auditability of data transactions [40]. This approach emphasizes transparency in access, rather than storing patient information directly on the blockchain. Additionally, IBM's MiPasa project, developed in response to the coronavirus pandemic, demonstrates blockchain's potential for recording and sharing health information, particularly related to antibody testing [41].

In summary, while blockchain may offer potential benefits in healthcare, its use for storing or managing highly sensitive personal data remains controversial. The reviewed literature underlines the importance of carefully designing hybrid architectures that combine blockchain with privacy-preserving technologies.

4.1.2. Education

Education has become a key public sector domain where blockchain solutions are being actively developed and tested. Blockchain offers a secure, tamper-proof system for issuing and verifying academic credentials. The University of Nicosia in Cyprus has implemented a system where academic certificates are authenticated through the Bitcoin blockchain, helping to reduce fraud and streamline the verification process for both students and employers [42]. Blockchain technology shows potential also in the area of digital identity management, simplifying access to educational resources and services [42]. Ngee Ann Polytechnic in Singapore is the first public educational institution in the country to use blockchain to verify the validity of its diplomas [44].

Furthermore, blockchain can enhance student innovation and creativity, enhancing manuscript submission, and ensuring timely and accurate peer reviews [43]. Finally, blockchain has supported the creation of distinct online learning platforms, facilitated the development of academic projects, and, most importantly, reduced fraud while enhancing security and privacy in the education sector [43].

4.1.3. Data Management

Blockchain has emerged as a promising solution for industries that demand high levels of data security, privacy, and trust [38]. Its suitability for managing and storing sensitive data, such as electronic medical records [36] and critical governmental information [45], highlights its potential to enhance the reliability and authenticity of data [46]. Blockchain offers significant improvements in public sector data

management, providing greater trust, transparency, and security [39]. In public-private partnerships, blockchain can play a key role in reducing information asymmetry, by protecting integrity of data and creating a tamper-proof record that traces data back to its origin. This capability is especially important in long supply chains or in managing sensitive information [46]. In the governmental sphere, where transparency, security, and efficiency are paramount, blockchain stands out as a disruptive force capable of ushering in a new era of digital governance [47].

4.1.4. Public finance

In the realm of public crowdfunding and fundraising, blockchain technology has emerged as a powerful tool for enhancing transparency, security, and efficiency. By leveraging blockchain, a decentralized fund can be established where anyone can contribute, ensuring that the management and allocation of these funds are transparent and trustworthy. Digital assets or tokens can be issued to represent equity in local development initiatives, facilitating the transfer of ownership stakes in projects. Smart contracts further streamline this process by creating a decentralized budgeting system, where fund allocation decisions are made through participant voting or upon reaching specific development milestones [48].

Blockchain also shows significant potential in revolutionizing agricultural financing by improving farmers' access to funds. A key application is the tokenization of physical assets like crops, livestock, and machinery, converting them into unique digital tokens. This transformation enhances their tradability, enabling their use as collateral in decentralized finance (DeFi) markets [49].

In the context of government accounting, blockchain technology is highlighted in several key areas, including auditing, budgetary and financial management, public procurement, contracts, accounting records, financial transactions, and asset transfers. The documented use cases suggest that blockchain can offer significant benefits, but challenges remain, particularly in terms of regulatory frameworks, scalability, performance, and the cultural shift required for adoption, especially given the scarcity of established use cases. Notable examples include Estonia's health platform and the Dubai Blockchain Strategy, both of which facilitate financial transactions via blockchain, a new model for recording land ownership in India, and a system for tracking imported goods into China [50].

4.1.5. E-voting

Although e-voting schemes have the potential to address challenges associated with traditional paper ballot elections, most existing systems rely on a centralized third party to manage the election process. This reliance creates vulnerabilities, susceptible to both internal and external threats. To address the limitations of centralized e-voting systems, many researchers have proposed leveraging blockchain technology to host e-voting schemes. Blockchain operates on an append-only model, where the immutable nature of its ledger discourages vote tampering and manipulation, once votes are recorded, they cannot be altered or erased (Clarke et al., 2023). Several countries have explored or implemented blockchain-based voting systems: Estonia has integrated blockchain into its voting process, and South Korea has successfully used blockchain-based e-voting in local elections [40].

However, achieving both ballot secrecy and election verifiability within blockchain-based voting remains a complex challenge. Blockchain's transparency can conflict with the need to keep votes confidential, and additional cryptographic techniques are often needed.

As a result, most current implementations focus on managing polls and surveys or on enhancing citizen participation in local and national decision-making processes, as discussed in Section 5, where some case studies are analysed. This evidence further highlights the limitations of blockchain for formal electoral purposes.

Table 2 summarises the application domains and descriptions of the most frequent blockchain use cases in the public sector.

4.2. Organizational and technical challenges in blockchain integration (RQ2)

To analyse the challenges encountered during blockchain adoption in the public sector, a specific framework is adopted [52], which classifies barriers into four categories.

- o Organizational Barriers.
- o Interaction-Specific Barriers.
- o Barriers Related to Perceived Characteristics of the Innovation.
- o Contextual Barriers.

The citations of articles addressing barriers to technology implementation, as investigated in the second research question, are summarized in Table A6 of the Appendix.

4.2.1. Organizational Barriers

Organizational barriers refer to internal obstacles within organizations, such as resistance to change, lack of technical expertise, and resource shortages. In the healthcare sector, the lack of understanding and expertise in blockchain technology among healthcare professionals leads to reluctance, implementation difficulties, and potential errors in using blockchain-based systems [53].

In the education sector, staff often lack the necessary technical skills, causing resistance to adoption and delays in implementation [43]. The high costs associated with blockchain implementation pose an additional obstacle, especially for institutions with limited budgets.

In public finance, a general lack of awareness about blockchain technology and its cost-effectiveness within public agencies hampers adoption [50]. Additionally, difficulties in replacing or adapting existing traditional systems present a significant challenge.

4.2.2. Interaction-Specific Barriers

Interaction-specific barriers refer to interoperability and integration issues between systems. In the healthcare sector, the absence of standardized protocols for integrating blockchain with existing systems hampers effective communication and data sharing between different institutions [54]. This issue negatively affects the efficiency of blockchain-based healthcare systems, limiting their ability to improve care quality and operational efficiency.

In public data management, the lack of interoperability represents a significant technical challenge. Ensuring that blockchain-based systems can effectively interact with existing infrastructures is important for large-scale adoption [39]. Without common standards, system fragmentation can lead to inefficiencies and hinder collaboration among public entities.

4.2.3. Barriers Related to Perceived Characteristics of the innovation

These barriers are related to user perceptions of the innovation's characteristics, such as complexity, compatibility, and relative advantage. Scalability issues emerge as one of the main technical barriers. Blockchain struggles to manage the vast amount of data generated by public systems, leading to slower transaction times and higher storage requirements [45,55].

In the healthcare sector, the sheer volume of data generated can slow down blockchain systems, especially when processing real-time information. This limits the technology's ability to be adopted on a large scale in sectors that require rapid data processing. In public data management, concerns about data security and privacy can negatively impact the perception of the innovation, hindering adoption [39].

4.2.4. Contextual Barriers

Contextual barriers refer to external obstacles, such as regulations, culture, and social environment. In e-voting, the lack of trust among voters reflects the cultural and social challenges of adopting blockchain technology. Despite the security and transparency guarantees offered,

many voters fear that the system could be vulnerable to manipulation or cyber-attacks, undermining participation and trust in the electoral process [56].

Additionally, the absence of a clear regulatory framework represents a significant barrier. The lack of industry-specific guidelines and regulations for blockchain in the public sector creates uncertainty and hampers widespread adoption. Policymakers and regulatory bodies must address legal and ethical concerns, ensure compliance with data privacy regulations, and establish clear standards for blockchain use [37,39,54,57].

In addition to the qualitative synthesis presented above, a supplementary quantitative overview is provided in Figs. A1 and A2, based on co-occurrence patterns identified through content analysis. Fig. A1 presents a heatmap of the estimated number of articles referring to either "Challenges" or "Barriers" in each sector, while Fig. A2 reports the proportion of studies mentioning each barrier type. These visualizations help illustrate the relative prominence of different barriers and highlight sectoral variations—for instance, the prevalence of organizational barriers in education or contextual concerns in healthcare.

4.3. Discussion on main results

Blockchain adoption in the public sector is shaped by a range of organizational, technical, and contextual challenges that vary across application domains. In Table 3, we summarize the types of barriers identified, following the framework from [52], which limit the adoption of blockchain in the public sector, suggesting instruments to overcome specific barriers. The "suggested instruments" reported in Table 3 are synthesized by the authors. They derive from our integrative reading of the cited studies and are organized according to the barrier typology of Cinar et al. [52]. We use them as theory-informed propositions, consistent with patterns observed in the literature, rather than as prescriptions validated by causal evidence. Interaction-related barriers are likely to benefit from interoperable standards, while perceived limitations like scalability or complexity call for further technological development. Contextual constraints, such as regulatory uncertainty or limited trust, suggest the need for broader institutional and societal efforts.

These propositions aim to make the literature's implications operational, but we do not claim causal identification. Future research should test these suggested instruments through comparative and longitudinal evaluations across sectors and institutional contexts to establish their effectiveness and boundary conditions.

Furthermore, the analysis of the literature highlights that each

Table 3
Barriers to blockchain adoption (RQ2).

Category	Specific Barriers	References	Suggested instruments
<i>Organizational Barriers</i>	Resistance to change; lack of technical expertise.	Luthra et al. [53]; Dash et al. [43]; Prux et al. [50]	Training and change management strategies
<i>Interaction-Specific Barriers</i>	Lack of interoperability and standardized protocols.	Rana et al. [54]; Mustafa et al. [39]	Introduction of interoperable standards
<i>Barriers Related to Perceived Characteristics of the Innovation</i>	Complexity, scalability issues, and privacy concerns.	Ali et al. [55]; Clavin et al. [45]; Mustafa et al. [39]	Technological development
<i>Contextual Barriers</i>	Lack of trust and unclear regulations.	Kassen [56]; Abdelhamid et al. [57]; Dhingra et al. [37]; Mustafa et al. [39]; Rana et al. [54]	Institutional policies, regulations

application domain faces specific types of barriers. Table 4 provides a summary of this characterization, aligning each domain with its most commonly associated challenges. Organizational obstacles, especially resistance to change and lack of technical expertise, are pervasive; for example, hospitals may struggle to implement blockchain-based systems due to insufficiently trained technical staff. Among interaction-specific barriers, interoperability issues are the most frequently reported, often requiring the development of technical standards and regulatory frameworks. Scalability concerns are prevalent across nearly all domains, while privacy issues are more prominent in areas involving sensitive personal data. Finally, contextual barriers are most often linked to regulatory uncertainty or the absence of clear legal frameworks.

At the same time, it is important to acknowledge the methodological limitations of the current literature. Most studies rely on conceptual models or exploratory case studies, which limits replicability and robustness. The literature tends to focus on proof-of-concept implementations in highly digitized countries, which may introduce publication bias and reduce generalizability to less mature contexts. Moreover, outcome indicators are often based on perceived variables - such as adoption intention or user satisfaction - rather than measurable performance improvements. A further indicator of the field's fragmentation is the dispersion of contributions across 33 different academic journals, with no single outlet accounting for more than 10 % of the total. Finally, a technical bias is evident, with limited attention to legal, political, or institutional dynamics.

Nonetheless, recent implementation experiences suggest that many of these barriers can be mitigated under favorable conditions. A growing body of evidence points to enabling factors that support effective adoption. These include technical readiness, inter-agency coordination, and strong governance structures. Estonia offers a particularly illustrative example: since 2012, its national eHealth system has incorporated blockchain to securely manage the medical records of over 1.3 million citizens. This model has improved data traceability, reduced administrative overhead, and increased public trust [40], demonstrating how a supportive ecosystem can transform blockchain from a conceptual innovation into a reliable public infrastructure.

Adoption patterns differ markedly across countries. Administrative capacity, legal frameworks, and institutional trust shape these dynamics. Berg, Davidson, & Potts [59] describe this tension as the "trust paradox": blockchain is most needed in low-trust environments - such as those with unreliable land registries - yet these are precisely the contexts where citizens may distrust governments' ability to implement such technologies effectively. Conversely, high-trust countries may have fewer incentives to adopt blockchain but are better positioned to do so successfully. These dynamics highlight the importance of developing context-sensitive strategies that integrate technological innovation with

transparency, institutional capacity building, and civic engagement.

5. Further case studies of blockchain adoption

To enrich the literature review with real-world case studies, this section analyzes key characteristics of blockchain adoption in selected initiatives. The data are drawn from an inventory of 270 blockchain use cases in the public sector, compiled by the European Commission's Joint Research Centre. Although this collection is neither exhaustive nor statistically representative [60], it provides substantial information on organizational features, service characteristics, and implementation status (CEU. JRC., 2022). The database does not report barriers or challenges and therefore cannot be used to validate RQ2; however it offers valuable descriptive evidenceto consolidate main answers to RQ1.

Following the previous analysis, we begin by describing the main application domains of the collected initiatives, as illustrated in Fig. 2. The two primary areas of application are General Public Services and Economic Affairs, which maps closely onto the SLR's most frequent application areas. General Public Services includes many activities related to the Data Management domain discussed earlier in Table 2, and several platforms for e-voting, primarily used for surveys and polls, designed to encourage stakeholder participation in both local and central government. Also this result is consistent with the SLR's finding that formal electoral uses remain limited. In addition, platforms for data

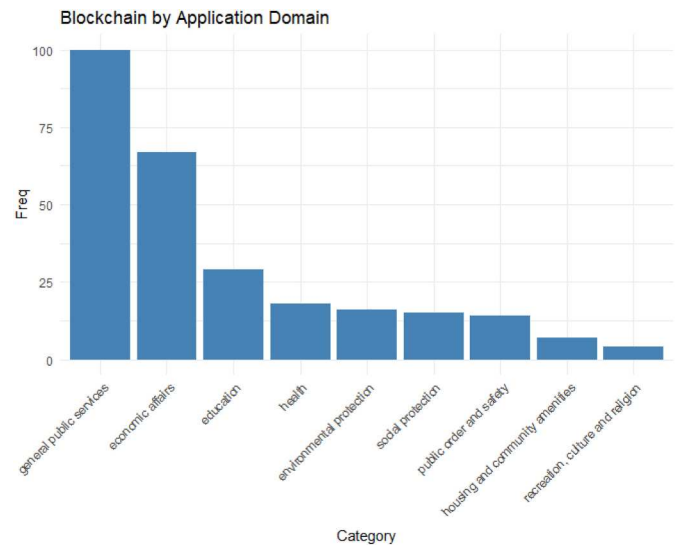


Fig. 2. Blockchain use cases by application domain.

Table 4

Use cases and associated barriers.

Application Domain	Organizational Barriers	Interaction-Specific Barriers	Perceived Characteristics of Innovation	Contextual Barriers	References
Healthcare	Resistance to change; lack of technical expertise.	Lack of interoperability and standardized protocols.	Scalability with large volumes of data; privacy concerns.	Lack of trust in blockchain systems.	Luthra et al. [53]; Dhingra et al. [37]; Lu et al. [38]; Mustafa et al. [39]; Rana et al. [54]
Education	Resistance to change; lack of technical expertise.	Interoperability challenges between systems.	Complexity of systems; scalability concerns.	Lack of clear regulations; cultural resistance.	Dash et al. [43]; Tan et al. [42]; Haneem et al. [44]; Rana et al. [54]
Data Management	Limited resources and technical expertise.	Lack of interoperability and integration standards.	Data security and privacy concerns; scalability issues.	Uncertainty in regulatory frameworks.	Lu et al. [38]; Mustafa et al. [39]; Du et al. [46]; Clavin et al. [45]; Anyanwu et al. [47]
Public Finance	Lack of awareness; resistance to change.	Integration difficulties with traditional systems.	Security and trust in financial systems.	Unclear regulations; public trust issues.	Radynskyy et al. [48]; Hung [49]; Prux et al. [50]; Kassen [56]; Abdelhamid et al. [57]
E-voting	Resistance to change.	Non-interoperable systems.	Scalability issues; privacy and security concerns.	Lack of voter trust; unclear legal frameworks.	Clarke et al. (2023)[58]; Verma & Sheel [40]; Kassen [56]; Rana et al. [54]

sharing, internal management, and procurement are also classified under this domain.

The Economic Affairs category encompasses various financial applications, mainly related to payments and international transactions. It also includes systems for goods tracking, copyright management, and data registration or notarization. Finally, the domains of Education and Health also emerge in the analysis, in line with previous findings from the literature review.

This cross-walk confirms the SLR's main domains, but it evidence also few minor areas (e.g., environmental protection, social protection, public order) that are rarely discussed in the literature but appear in practice, suggesting topics for future inquiry. A comparison between SLR results and the case studies analysis is synthesized in Table 5.

Additional insights from the data analysis concern the geographical distribution of blockchain initiatives, the responsible organizations, and their implementation status.

As to the implementation state (Fig. 3), most initiatives are still in the pilot phase (63.7 %), while 46 projects are already reported as implemented. This evidence helps explain occasional misalignments between the SLR (which prioritizes published, implemented activities) and the case inventory (which also lists pilots and planned projects). Notably, about 85 % of implemented cases fall within the domains identified by the SLR for RQ1, reinforcing the external consistency of the literature-derived patterns. In details, in the Health domain, beyond Estonia's well-known e-Health Record, blockchain technology has been implemented during the COVID-19 pandemic for green pass management (San Marino) and cold chain vaccine monitoring (United Kingdom).

In the Education domain, all seven identified initiatives focus on certification and credential validation processes, as it emerged in the literature review.

Regarding the e-voting domain, the database reports four implemented blockchain-based systems—in Russia, Poland, Portugal, and Estonia—used primarily for organizing surveys and polls or monitoring electoral exit polls.

Seven implemented blockchain applications relate to financial services; however, most are designed to provide benefits or discounts to low-income households. Notably, in Poland, a blockchain system was launched to track the sale and distribution of Polish treasury or government savings bonds. Meanwhile, in the municipality of Zermatt, Switzerland, where taxpayers are officially allowed to pay taxes in Bitcoin, local authorities have partnered with one of the country's major crypto financial service providers.

Finally, Figs. 4 and 5 show the distribution of the entire dataset by country and by responsible organization, respectively. A group of countries—including Italy, the Netherlands, Spain, the United Kingdom, and Germany—along with the European Union, appears particularly active in blockchain adoption. Since the data do not result from a comprehensive census, these geographical distributions may reflect differences in data collection systems across countries. While the distribution by country highlights where blockchain-related initiatives are most frequently reported, these figures alone do not account for differences in national policy contexts or levels of institutional trust. Estonia, often cited as a high-trust, digitally advanced country, adopts

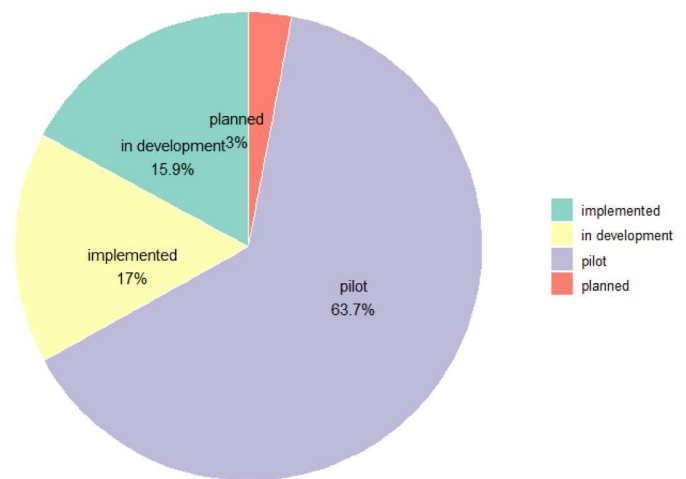


Fig. 3. Blockchain use cases by status.

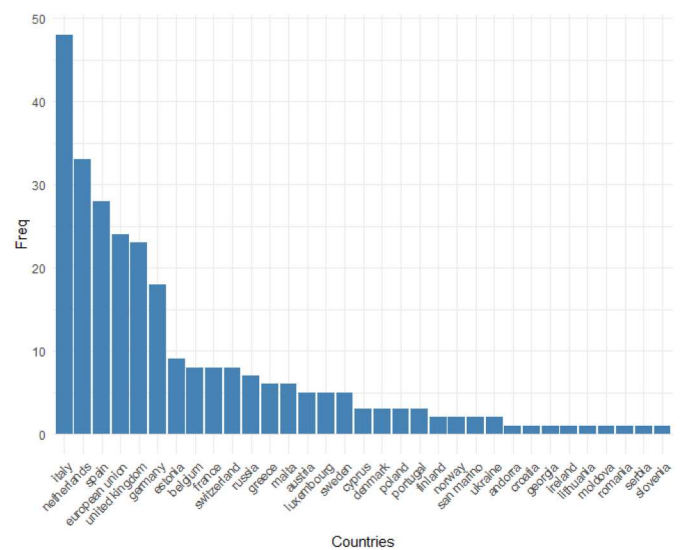


Fig. 4. Blockchain use cases by country.

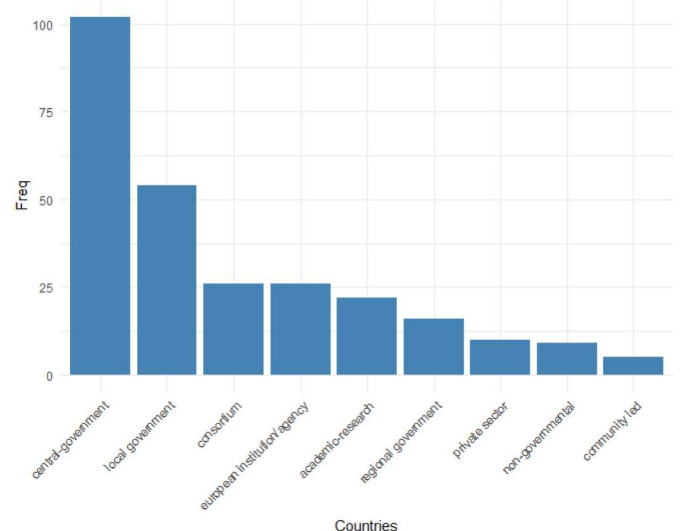


Fig. 5. Blockchain use cases by responsible organization.

Table 5

– Synthesis of comparison between SLR results and case studies.

SLR domains (RQ1)	JRC Category	Typical Implementation in Inventory
Health	Health	Access/audit logs, document trails; supply chain.
Education	Education	Credential issuance and digital identities
Data	General Public	E-procurement records, data-sharing
Management	Services	platforms, notarization/registries
Public Finance	Economic Affairs	targeted benefits, asset tracking, payments
e-Voting	General Public	Polls, consultations, exit-poll support (not general elections)
	Services	

blockchain as an extension of its already mature e-governance infrastructure. Here, blockchain reinforces existing trust. In contrast, in countries where institutional trust may be lower or where corruption perceptions are higher, blockchain is sometimes introduced as a compensatory mechanism to increase transparency and traceability. These qualitative contrasts suggest that regional variations in blockchain adoption are not only a matter of frequency but also of purpose and institutional context.

Finally, the most prominent organizations driving blockchain adoption are central and local governments, signaling the relevance of institutional support as enabler in the blockchain adoption.

While the available case studies do not allow for a systematic cross-country comparison of success factors, some recurring enabling conditions can be inferred from the evidence reviewed. These include the presence of strong institutional support, pre-existing digital infrastructure, public-private partnerships, and a clear legal or regulatory framework. In several cases, blockchain adoption was facilitated by limiting its initial use to low-risk administrative tasks—such as surveys, credential verification, or data audit trails—before considering more sensitive applications. These observations are exploratory and should be interpreted with caution, given the variability in data quality and reporting standards across countries. Based on the case studies discussed, some preliminary enabling conditions for successful blockchain adoption in the public sector can be identified, as summarized in Table 6. These factors are not meant to be exhaustive or universally applicable but rather reflect common elements observed in the reviewed examples. They provide a basis for future empirical work on the conditions that facilitate or hinder blockchain implementation in different administrative and national contexts.

6. Conclusions and future agenda

This paper has examined how blockchain technology is utilized across various public sector domains and identified the main organizational and technical barriers hindering its adoption. The responses to our research questions indicate that while blockchain offers substantial opportunities to enhance transparency, security, and efficiency in public services, significant challenges impede its widespread deployment. These challenges vary depending on the context and application area.

Our contribution is to foreground an economic–organizational perspective on public-sector adoption, to synthesize evidence from 37 peer-reviewed studies, and to integrate a data-driven thematic analysis

with a qualitative appraisal of source rigor. Furthermore, the literature review has been complemented through a comparison with real-world case studies, based on a dataset of 270 blockchain initiatives adopted by the public sector in Europe. The findings reveal that many initiatives are still in early development phases, and their application areas suggest a predominantly experimental use in non-core administrative functions. The most notable exception is Estonia's e-Health platform, which stands out as a mature and integrated implementation.

Blockchain adoption in the public sector appears to be in a critical transitional phase, unlike the private sector, where it is advancing rapidly toward technological maturity in specific applications. The SLR and the case inventory indicate that public-sector adoption concentrates on some areas of application, such as auditability, credentialing, notarization, procurement, payments, and tracking applications, with initiatives concentrated in low-risk activities. This suggests a cautious approach to blockchain implementation in the public sector.

The practical implications of our findings are extensive. Effective adoption of blockchain in the public sector requires tailored approaches that consider the unique challenges of each sector. Public decision-makers must recognize that there is no one-size-fits-all solution, and overcoming the identified barriers is critical to fully leveraging the technology's potential. Significant investment in technical training and infrastructure is needed. Developing well-defined regulatory frameworks that address privacy, data protection, and stakeholder accountability is also necessary. Promoting public trust through transparency and education can effectively overcome cultural and social barriers.

At the same time, several limitations constrain what can currently be concluded from the academic literature. For instance, the way public sector projects are reported remains highly heterogeneous and inconsistent. Many articles reference multiple initiatives without standardized naming conventions, making cross-study aggregation methodologically challenging. This points to an important avenue for future research, which should aim to establish more coherent documentation practices and case-based evidence. Similarly, the identification of adoption barriers in this study is based on how they are conceptualized and reported in scholarly literature. Further empirical studies are needed to explore how such challenges unfold in concrete project implementations.

6.1. Towards a research Agenda

Building upon the findings of this review, several avenues for future research emerge, aiming to address existing gaps and deepen the understanding of blockchain adoption in the public sector. Comparative studies between public and private sectors could help identify the distinct barriers and enablers that influence adoption dynamics in different institutional settings, offering insights into sector-specific challenges and strategic responses. In addition, longitudinal research designs may provide valuable perspectives on how public organizations evolve in their use of blockchain over time, offering dynamic insight into the resolution of implementation hurdles.

Overall, the findings provide a coherent answer to the research questions guiding this study. Regarding RQ1, the analysis reveals that blockchain integration in the public sector is concentrated in a limited set of domains - such as healthcare, education, data management, public finance, and e-voting - where implementation remains largely experimental and focused on low-risk administrative functions. With respect to RQ2, the review identifies four main categories of barriers (organizational, interaction-specific, innovation-related, and contextual) that jointly explain the uneven pace of adoption across these domains. The comparative analysis with European case studies confirms that the degree of digital maturity, regulatory clarity, and institutional trust significantly influence how these challenges manifest and are addressed in practice. These insights consolidate the analytical bridge between the two research questions, linking observed implementation patterns (RQ1) to their underlying constraints and enabling factors (RQ2).

A sectoral lens also appears particularly promising. In the field of

Table 6
– Potential enablers for blockchain adoption.

Enabling Condition	Description	Example(s)
Institutional support	Strong commitment from national or local governments facilitates adoption.	Estonia (eHealth), South Korea (e-voting), Zermatt (taxes in BTC)
Digital infrastructure	Existing IT systems and digital governance maturity ease blockchain integration.	Estonia (national digital ID and health systems)
Public-private partnerships	Collaborations with private tech providers provide resources and technical know-how.	Zermatt (blockchain tax payment via crypto firm)
Regulatory clarity or experimental frameworks	Adoption is eased when there is a clear legal environment or regulatory sandbox.	South Korea (pilots in regulated settings)
Use in low-risk or administrative domains	Initial adoption in non-sensitive areas reduces implementation risk and builds institutional trust.	Education (credentialing), local polls, surveys
Stakeholder engagement	Early involvement of users (citizens, employees) enhances acceptance and reduces resistance to change.	Participatory budgeting and consultations in local governments

healthcare, future research could examine organizational models for integrating blockchain into both centralized and decentralized systems, with a focus on data security and interoperability. In the education sector, further work is needed on the development of globally interoperable solutions for academic credential verification, especially concerning standardization and cross-border recognition. When it comes to data management, studies could prioritize the design of technical standards and protocols that enable interoperability between public and private blockchain infrastructures, particularly in areas where multiple platforms must interact. In the domain of public finance, research may assess the role of blockchain in improving budget transparency and investigate the technical feasibility of large-scale deployments in financial administration. About e-voting, further investigation is needed to explore mechanisms for strengthening voter trust in blockchain-based electoral systems, considering diverse legal, cultural, and institutional environments.

Moreover, the human and behavioural dimensions of blockchain adoption remain underexplored. Systematic studies on resistance to change, digital literacy gaps, and other socio-cultural factors could enhance our understanding of how public servants and citizens interact with blockchain-enabled services, and under what conditions adoption is more likely to succeed.

Although blockchain technology offers promising opportunities to improve transparency, security, and efficiency in the public sector, its adoption is conditioned by a complex interplay of organizational, technical, and contextual variables. Advancing research through interdisciplinary collaboration and empirical investigation can support more nuanced, evidence-based approaches, contributing to the effective and sustainable implementation of blockchain in diverse public service domains.

CRedit authorship contribution statement

Angelo Murano: Writing – original draft, Methodology, Investigation, Data curation, Conceptualization. **Bruna Bruno:** Writing – review & editing, Supervision. **Vincenzo Vespri:** Writing – review & editing, Supervision.

Appendix A. Supplementary data

Supplementary data to this article can be found online at <https://doi.org/10.1016/j.seps.2025.102364>.

Data availability

Data will be made available on request.

References

- [1] Kane E. Is blockchain a general purpose technology? Soc Sci Res Netw 2017, marzo 11. <https://doi.org/10.2139/ssrn.2932585> [SSRN Scholarly Paper]. Rochester, NY.
- [2] Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. <https://doi.org/10.48550/ARXIV.1906.11078>; 2019.
- [3] Cagigas D, Clifton J, Diaz-Fuentes D, Fernández-Gutiérrez M. Blockchain for public services: a systematic literature review. IEEE Access 2021;9:13904–21. <https://doi.org/10.1109/ACCESS.2021.3052019>.
- [4] Allesie D, Sobolewski M, Vaccari L. Blockchain for digital government an assessment of pioneering implementations in public services. <https://doi.org/10.13140/RG.2.2.34874.85449>; 2019.
- [5] Batubara FR, Ubacht J, Janssen M. Challenges of blockchain technology adoption for e-government: a systematic literature review. Proceedings of the 19th annual international conference on digital government research: governance in the data Age. Delft The Netherlands: ACM; 2018. p. 1–9. <https://doi.org/10.1145/3209281.3209317>.
- [6] Riyoldi R, Muhtar EA, Karlina N. The potential use of blockchain technology in public service A systematic literature review. Preprints 2023, novembre 17. <https://doi.org/10.20944/preprints202311.1150.v1>.
- [7] Tan E, Mahula S, Crompvoets J. Blockchain governance in the public sector: a conceptual framework for public management. Gov Inf Q 2022;39(1):101625. <https://doi.org/10.1016/j.giq.2021.101625>.
- [8] Walker RM, Avellaneda CN, Berry FS. Exploring the diffusion of innovation among high and low innovative localities: a test of the berry and berry model. Public Manag Rev 2011;13(1):95–125. <https://doi.org/10.1080/14719037.2010.501616>.
- [9] Moher D, Liberati A, Tetzlaff J, Altman DG. Linee guida per il reporting di revisioni sistematiche e meta-analisi: il PRISMA Statement. Open access 2015;7(6).
- [10] Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inf 2019;36:55–81. <https://doi.org/10.1016/j.tele.2018.11.006>.
- [11] Risius M, Spohrer K. A blockchain research framework. Business & Information Systems Engineering 2017;59(6):385–409. <https://doi.org/10.1007/s12599-017-0506-0>.
- [12] D'Este P, Iammarino S, Savona M, von Tunzelmann N. What hampers innovation? Revealed barriers versus deterring barriers. Res Pol 2012;41(2):482–8. <https://doi.org/10.1016/j.respol.2011.09.008>.
- [13] Shavinina LV. The international handbook on innovation. first ed. Amsterdam Boston: Elsevier Science; 2003.
- [14] Borins SF. The persistence of innovation in government. Brookings institution press with ash Center for democratic governance and innovation. 2014.
- [15] Torugsa N, Ann, Arundel A. Complexity of Innovation in the public sector: a workgroup-level analysis of related factors and outcomes. Public Manag Rev 2016; 18(3):392–416. <https://doi.org/10.1080/14719037.2014.984626>.
- [16] Balzarova M, Dyer C, Falta M. Perceptions of blockchain readiness for fairtrade programmes. Technol Forecast Soc Change 2022;185:122086. <https://doi.org/10.1016/j.techfore.2022.122086>.
- [17] Li Y, Su DA, Mardani A. Digital twins and blockchain technology in the industrial internet of Things (IIoT) using an extended decision support system model: industry 4.0 barriers perspective. Technol Forecast Soc Change 2023;195:122794. <https://doi.org/10.1016/j.techfore.2023.122794>.
- [18] Liyanaarachchi G, Viglia G, Kurtaliqui F. Addressing challenges of digital transformation with modified blockchain. Technol Forecast Soc Change 2024;201: 123254. <https://doi.org/10.1016/j.techfore.2024.123254>.
- [19] Singh AK, Kumar VRP, Shoaib M, Adebayo TS, Irfan M. A strategic roadmap to overcome blockchain technology barriers for sustainable construction: a deep learning-based dual-stage SEM-ANN approach. Technol Forecast Soc Change 2023; 194:122716. <https://doi.org/10.1016/j.techfore.2023.122716>.
- [20] Sternberg HS, Hofmann E, Roeck D. The struggle is real: insights from a supply chain blockchain case. J Bus Logist 2021;42(1):71–87. <https://doi.org/10.1111/jbl.12240>.
- [21] Moura L M F de, Brauner DF, Janissek-Muniz R. Blockchain and a technological perspective for public administration: a systematic review. Revista de Administração Contemporânea 2020;24:259–74. <https://doi.org/10.1590/1982-7849rac2020190171>.
- [22] Rodríguez Bolívar MP, Scholl HJ. Mapping potential impact areas of Blockchain use in the public sector. Inf Polity 2019;24(4):359–78. <https://doi.org/10.3233/IP-190184>.
- [23] Trequattrini R, Palmaccio M, Turco M, Manzari A. The contribution of blockchain technologies to anti-corruption practices: a systematic literature review. Bus Strat Environ 2024;33(1):4–18.
- [24] Zhang Y, Tavalaei MM, Parry G, Zhou P. Evolution or involution? A systematic literature review of organisations' blockchain adoption factors. Technol Forecast Soc Change 2024;208:123710. <https://doi.org/10.1016/j.techfore.2024.123710>.
- [25] Kraus S, Breier M, Dasí-Rodríguez S. The art of crafting a systematic literature review in entrepreneurship research. Int Enterpren Manag J 2020;16(3):1023–42. <https://doi.org/10.1007/s11365-020-00635-4>.
- [26] Tranfield D, Denyer D, Smart P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. Br J Manag 2003;14(3):207–22. <https://doi.org/10.1111/1467-8551.00375>.
- [27] Paul J, Merchant A, Dwivedi YK, Rose G. Writing an impactful review article: what do we know and what do we need to know? J Bus Res 2021;133:337–40. <https://doi.org/10.1016/j.jbusres.2021.05.005>.
- [28] Webster J, Watson RT. Analyzing the past to prepare for the future: writing a literature review. MIS Q 2002;26(2):xiii–xxiii.
- [29] Keupp MM, Palmié M, Gassmann O. The strategic management of innovation: a systematic review and paths for future research. Int J Manag Rev 2012;14(4): 367–90. <https://doi.org/10.1111/j.1468-2370.2011.00321.x>.
- [30] Lamb CW. Public sector marketing is different. Bus Horiz 1987;30(4):56–60. [https://doi.org/10.1016/0007-6813\(87\)90066-8](https://doi.org/10.1016/0007-6813(87)90066-8).
- [31] Boyne GA. Public and private management: what's the difference? J Manag Stud 2002;39(1):97–122.
- [32] Peters BG, Pierre J. Governance without government? Rethinking public administration. J Publ Adm Res Theor 1998;8(2):223–43. <https://doi.org/10.1093/oxfordjournals.jpart.a024379>.
- [33] Rusaw AC. Administrative leadership in the public sector. Public Adm Rev 2009;69 (3):551–3. <https://doi.org/10.1111/j.1540-6210.2009.02003.x>.
- [34] Farnham D, Horton S. The new public service managerialism: an assessment. In: Farnham D, Horton S, Di Ac, editors. Managing the new public services. London: Macmillan Education UK; 1993. p. 237–54. https://doi.org/10.1007/978-1-349-22646-7_11.
- [35] Baldwin JN. Public versus private: not that different, not that consequential. Public Pers Manag 1987;16(2):181–93. <https://doi.org/10.1177/009102608701600209>.
- [36] Zhang R, Xue R, Liu L. Security and privacy for healthcare blockchains. IEEE Transactions on Services Computing 2022;15(6):3668–86. <https://doi.org/10.1109/TSC.2021.3085913>.
- [37] Dhingra S, Raut R, Gunasekaran A, Rao Naik BK, Masuna V. Analysis of the challenges for blockchain technology adoption in the Indian health-care sector.

- J Model Manag 2023;19(2):375–406. <https://doi.org/10.1108/JM2-09-2022-0229>.
- [38] Lu L, Liang C, Gu D, Ma Y, Xie Y, Zhao S. What advantages of blockchain affect its adoption in the elderly care industry? A study based on the technology–organisation–environment framework. *Technol Soc* 2021;67. <https://doi.org/10.1016/j.techsoc.2021.101786>. Scopus.
- [39] Mustafa G, Rafiq W, Jhamat N, Arshad Z, Rana FA. Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management* 2024. <https://doi.org/10.1108/IJLMA-08-2023-0172>. ahead-of-print(ahead-of-print).
- [40] Verma S, Sheel A. Blockchain for government organizations: past, present and future. *Journal of Global Operations and Strategic Sourcing* 2022;15(3):406–30. <https://doi.org/10.1108/JGOSS-08-2021-0063>.
- [41] Bustamante P, Cai M, Gomez M, Harris C, Krishnamurthy P, Law W, Weiss M. Government by code? Blockchain applications to public sector governance. *Frontiers in Blockchain* 2022;5. <https://doi.org/10.3389/fbloc.2022.869665>.
- [42] Tan E, Lerouge E, Du Caju J, Du Seuil D. Verification of education credentials on European Blockchain Services Infrastructure (EBSI): action research in a cross-border use case between Belgium and Italy. *Big Data and Cognitive Computing* 2023;7(2):79. <https://doi.org/10.3390/bdcc7020079>.
- [43] Dash MK, Panda G, Kumar A, Luthra S. Applications of blockchain in government education sector: a comprehensive review and future research potentials. *Journal of Global Operations and Strategic Sourcing* 2022;15(3):449–72. <https://doi.org/10.1108/JGOSS-09-2021-0076>.
- [44] Haneem F, Abu H, Kama N, Zalbiha N, Ghazali R, Mahmood Y. Recent progress of blockchain initiatives in government. *Int J Adv Comput Sci Appl* 2020;11(11). <https://doi.org/10.14569/IJACSA.2020.0111144>.
- [45] Clavin J, Duan S, Zhang H, Janeja VP, Joshi KP, Yesha Y, Li JD. Blockchains for government: use cases and challenges. *Digital Government: research and Practice*. 2020. <https://doi.org/10.1145/3427097>. 1(3). Scopus.
- [46] Du Y, Yuan J, Wang S, Liu Y, Zeng N. Leveraging blockchain to anchor information for supervision in PPP projects: a conceptual framework. *Eng Construct Architect Manag* 2024. <https://doi.org/10.1108/ECAM-07-2023-0758>. ahead-of-print(ahead-of-print).
- [47] Anyanwu A, Dawodu SO, Omotosho A, Akindote OJ, Ewuga SK, Anyanwu A, Ewuga SK. Review of blockchain technology in government systems: applications and impacts in the USA. *World Journal of Advanced Research and Reviews* 2023; 20(3):863–75. <https://doi.org/10.30574/wjarr.2023.20.3.2553>.
- [48] Radynskyy S, Ratynskiy V, Diachenko N, Diachenko V, Krupka A, Lobodina Z, Bendih V. Improving the financing mechanism for the development of local communities based on the use of digital technologies. *Eur J Enterprise Technol* 2024;2(13):35–46. <https://doi.org/10.15587/1729-4061.2024.300908>. 128.
- [49] Hung. The curious case of blockchain in rural China: unravelling power, profit, and surveillance. <https://doi.org/10.1177/20539517241259674>; 2024.
- [50] Prux PR, Momo F da S, Melati C. Opportunities and challenges of using blockchain technology in government accounting in Brazil. *BAR - Brazilian Administration Review* 2021;18:e200109. <https://doi.org/10.1590/1807-7692bar2021200109>.
- [51] Adams RJ, Smart P, Huff AS. Shades of Grey: guidelines for working with the Grey Literature in systematic reviews for management and organizational studies. *Int J Manag Rev* 2017;19(4):432–54. <https://doi.org/10.1111/ijmr.12102>.
- [52] Cinar E, Trott P, Simms C. A systematic review of barriers to public sector innovation process. *Public Manag Rev* 2019;21(2):264–90. <https://doi.org/10.1080/14719037.2018.1473477>.
- [53] Luthra S, Janssen M, Rana NP, Yadav G, Dwivedi YK. Categorizing and relating implementation challenges for realizing blockchain applications in government. *Inf Technol People* 2022;36(4):1580–602. <https://doi.org/10.1108/ITP-08-2020-0600>.
- [54] Rana NP, Dwivedi YK, Hughes DL. Analysis of challenges for blockchain adoption within the Indian public sector: an interpretive structural modelling approach. *Inf Technol People* 2022;35(2):548–76. <https://doi.org/10.1108/ITP-07-2020-0460>. Scopus.
- [55] Ali O, Jaradat A, Kulakli A, Abuhaleme A. A comparative Study: blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* 2021;9: 12730–49. <https://doi.org/10.1109/ACCESS.2021.3050241>. Scopus.
- [56] Kassen M. Politicization of e-voting rejection: reflections from Kazakhstan. *Transforming Gov People, Process Policy* 2020;14(2):305–30. <https://doi.org/10.1108/TG-11-2019-0106>. Scopus.
- [57] Abdelhamid IR, Halim ITA, Ali AE-MA, Ibrahim IA. A survey on blockchain for intelligent governmental applications. *Indonesian Journal of Electrical Engineering and Computer Science* 2023;31(1):501–13. <https://doi.org/10.11591/ijeecs.v31.i1.pp501-513>.
- [58] Clarke. Applied sciences | free full-text | online voting scheme using IBM cloud-based hyperledger fabric with privacy-preservation. *Recuperato* 2023;18 luglio 2024. da, <https://www.mdpi.com/2076-3417/13/13/7905>.
- [59] Berg C, Davidson S, Potts J. Understanding the blockchain economy: an introduction to institutional cryptoeconomics. Edward Elgar Publishing; 2019.
- [60] Rodriguez Müller AP, Martin Bosch J, Tangi L. An overview of the expected public values arising from blockchain adoption in the European public sector. *Int J Public Sect Manag* 2025;38(1):53–76. <https://doi.org/10.1108/ijpsm-12-2023-0363>.

Angelo Murano is a Ph.D. candidate in Economics at the University of Salerno. His research focuses on the Economics of Innovation and the Economics of Institutions, with a specific interest in how technology can support institutional decision-making and policy design in the public sector.

Bruna Bruno is a Full Professor of Economics at the University of Salerno. Her research interests include labor economics, institutional economics, and technological innovation.

Vincenzo Vespri is a Full Professor of Mathematics at the University of Florence. His research spans various areas of mathematics, statistics, and computer science.



sustainability



Article

Incentives for Sustainable Governance in Blockchain-Based Organizations

Bruna Bruno, Angelo Murano and Vincenzo Vespri

Special Issue

Digital Innovation in Sustainable Economics and Business

Edited by

Dr. Bruna Bruno, Dr. Marisa Faggini and Dr. Anna Parziale



<https://doi.org/10.3390/su17219728>

Article

Incentives for Sustainable Governance in Blockchain-Based Organizations [†]

Bruna Bruno ^{1,*} , Angelo Murano ¹  and Vincenzo Vespri ² 

¹ Department of Economics and Statistics, University of Salerno, via Giovanni Paolo II, 84084 Fisciano, Italy; amurano@unisa.it

² Department of Mathematics and Computer Science “Ulisse Dini”, University of Florence, Viale Morgagni 67/a, 50134 Firenze, Italy; vincenzo.vespri@unifi.it

* Correspondence: brbruna@unisa.it

[†] This paper is an extended version of our paper published in Murano, A.; Bruno, B.; Vespri, V. Incentive Compatibility in Consensus Protocols and DAOs: A Game-Theoretic Approach. In Proceedings of the Distributed Ledger Technology Workshop 2024, Proceedings of the Sixth Distributed Ledger Technology Workshop (DLT 2024), Turin, Italy, 14–15 May 2024.

Abstract

This study analyzes how blockchain technology can be interpreted through an economic perspective, viewing network nodes as rational agents whose strategic behavior affects the efficiency and sustainability of decentralized systems. Using a multi-player non-cooperative game with complete but imperfect information, we model validators’ decisions in voting-based consensus mechanisms and compare alternative incentive configurations through simulation results. The analysis shows how variations in reward schemes influence validators’ behavior and consensus reliability. Extending the framework to Decentralized Autonomous Organizations (DAOs), the study explores how blockchain-based incentives can enhance participation, accountability, and decentralized governance. The findings highlight that incentive design plays a decisive role in aligning individual motivations with collective goals, ensuring both network integrity and long-term sustainability. Overall, this study connects economic theory with blockchain governance, extending its relevance to business and organizational contexts beyond cryptocurrencies.

Keywords: incentive compatibility; game-theoretic approach; blockchain governance



Academic Editor: Fabrizio D’Ascenzo

Received: 30 September 2025

Revised: 28 October 2025

Accepted: 30 October 2025

Published: 31 October 2025

Citation: Bruno, B.; Murano, A.; Vespri, V. Incentives for Sustainable Governance in Blockchain-Based Organizations. *Sustainability* **2025**, *17*, 9728. <https://doi.org/10.3390/su17219728>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Blockchain technology has drawn increasing interest from both computer scientists and economists recently, initially because of its role in supporting cryptocurrencies, such as Bitcoin [1], the most well-known example of a blockchain-based decentralized cryptocurrency. It is now widely recognized, however, as a general-purpose technology [2] with potential applications far beyond monetary systems. Blockchain solutions are being adopted in diverse sectors, including supply chain management, healthcare, digital identity, finance, education, environmental governance, and both private and public administration, where their decentralized structure enhances transparency, security, and efficiency [3].

In supply chain logistics, blockchain technology offers the advantages of reducing supply chain fraud and enhancing traceability because it ensures transparent records and accountability [4]. In the healthcare domain, blockchain enables the safe and efficient sharing of medical records and safeguards the confidentiality of health data [5]. Similarly, blockchain-enabled digital identity systems offer decentralized and resilient platforms for

verifying individual identities, thereby lowering the risk of identity theft and strengthening personal control over one's private data [6]. In these settings, blockchain adoption not only fosters transparency and curtails opportunistic behavior but also supports greater economic and environmental sustainability. For instance, in supply chains, blockchain-enabled traceability can help minimize waste, streamline logistics operations, and improve energy efficiency, directly contributing to lower emissions and reduced overall coordination costs.

Participation in blockchain networks relies on incentive mechanisms. In cryptocurrency-based blockchains, such incentives usually take the form of cryptocurrency rewards. In non-cryptocurrency applications, participation is encouraged by rewards or digital assets. For instance, in supply chains that leverage blockchain technology, participants are rewarded with tokens for providing precise and timely data inputs. This practice underpins the overall efficiency and trustworthiness of the supply chain [7]. These incentive structures not only safeguard the system's integrity but also promote cooperative behavior among stakeholders. At the same time, incentive design must consider long-term economic and environmental sustainability, favoring consensus protocols, such as Proof-of-Stake or hybrid variants, that limit energy consumption while ensuring efficiency and fairness.

This study aims to integrate key blockchain features into an economic framework. An economic perspective can complement the extensive body of research developed within computer science and provide valuable insights into decision-making and the management of incentive problems. Such interdisciplinary integration is particularly important in applications where opportunistic behavior may emerge. From an economic standpoint, blockchain nodes are viewed as agents with their own preferences and incentives, capable of free-riding. In economic terms, a free-rider is someone who benefits from public goods without bearing any of the associated costs. If not properly addressed, free-riding undermines not only the integrity of decentralized systems but also their economic sustainability, as it increases overall their maintenance costs. From an environmental perspective, inefficiencies in participation mechanisms may amplify energy waste and reduce the comparative advantage of blockchain solutions over centralized alternatives.

Blockchain technology has revolutionized various industries by introducing decentralized systems that enhance transparency, security, and efficiency [8]. Previous research has extensively analyzed incentive mechanisms within blockchain networks, focusing on how they influence participant behavior and network performance. These analyses often employ game theory to model strategic interactions among network participants, considering both economic incentives and the ethical and legal challenges that arise in decentralized systems. The present study contributes to this body of literature by analyzing different reward mechanisms designed to align the incentives of self-interested agents seeking to maximize their utility functions. The contribution is primarily analytical, supported by formal mathematical proofs and validated through simulation results. Compared to existing research [9], this study extends the evaluation of incentive compatibility constraints by explicitly considering the intrinsic satisfaction deriving from adherence to or sabotage of organizational stability, beyond simple extrinsic rewards.

Furthermore, by extending the concept of incentive compatibility to organizational frameworks structured as DAOs, this study investigates how incentive mechanisms can support decentralized governance systems, while considering economic implications and legal constraints. This extension is essential for understanding how authority can be decentralized in organizations, reflecting the distributed nature of blockchain technology itself. The analysis illustrates how reward structures and blockchain-based organizational models can be designed to ensure economic efficiency, reduce energy costs, and enhance organizational resilience.

Overall, this study seeks to understand how economic incentives can foster forms of decentralized governance that are both efficient and sustainable. The research question is formulated as follows: *How can incentive design promote sustainable governance in decentralized organizations?*

This study is a revised and expanded version of a paper entitled “Incentive Compatibility in Consensus Protocols and DAOs: A Game-Theoretic Approach,” which was presented at the 6th Distributed Ledger Technology Workshop (DLT2024), Turin (Italy) [10]. In this extended version, the incentive compatibility issue within non-cryptocurrency blockchain is explored in its implications for Decentralized Autonomous Organizations (DAOs). DAOs are explored not only as a technological innovation but as a novel approach to economic organization and governance. While the technical aspects of DAOs and vulnerabilities, like the Reentrancy Attack, have been thoroughly explored in the IT literature, there is a noticeable gap in the analysis of their economic and legal implications.

The remainder of this study is organized as follows: Section 2 presents and discusses case studies on free-riding within blockchain technology. Section 3 reviews the economic literature on blockchain technologies. Section 4 analyzes the incentive compatibility of two alternative reward schemes for voting-based consensus mechanisms. Section 5 examines governance challenges within DAOs and their role in the blockchain ecosystem. Section 6 concludes with our key findings and policy implications.

2. Free-Riding and the Blockchain: Some Case Studies

Free-riding is a well-established topic in the literature on public economics [11] and can be analyzed through a game-theoretic lens. In a simplified two-player economy, the socially optimal Pareto outcome diverges from the Nash equilibrium because each participant has an incentive to under-contribute.

In decentralized blockchain environments, the coordination of multiple autonomous agents creates similar opportunities for free-riding. Without a central authority to monitor and enforce compliance, participants may strategically withhold information or misreport transactions. These vulnerabilities are particularly significant in applications, such as supply chain management, public record-keeping, and collective decision-making. In blockchain-enabled supply chains, participants may underreport transactions or distort information to gain an advantage while still benefiting from the shared infrastructure. In decentralized finance (DeFi), free-riding can emerge through collusion or strategic inaction, reducing accountability. Similarly, in blockchain-based identity, certification, or procurement systems, actors may submit false or redundant verification requests, undermining trust and efficiency. In the absence of the direct oversight characteristic of centralized systems, such practices can erode the integrity and trust that are fundamental to blockchain operations. Free-riding also generates inefficiencies and raises operating costs, potentially making blockchain networks economically unsustainable unless effective incentive mechanisms are in place [12]. Simulations confirm that the level of honest participation in a blockchain system is critically dependent on the design of the incentives and highlight the fragility of the cooperative balance required to sustain blockchain networks [13].

Economics addresses problem-solving and decision-making through an emphasis on agent behavior, dynamic interactions, and systemic interdependencies. By contrast, computer science focuses on system architecture, algorithmic optimization, and information processing, typically dealing with well-defined and logically structured problems to ensure technical efficiency and precision. Bridging these two perspectives is crucial for designing blockchain solutions that combine technical robustness with long-term economic viability. Computer science typically models agents in dichotomous terms, as “honest” or “malicious”

and shows that protocols remain reliable as long as the proportion of malicious participants remains below a defined threshold [14].

The 2016 attack on the Decentralized Autonomous Organization (DAO) serves as a significant illustration of blockchain's ethical and security challenges. Exploiting a flaw in the code of the DAO, a hacker diverted 3.6 million Ether (approximately 50 million U.S. dollars) into a personal account. The DAO represented an early experiment in blockchain-based governance, designed to democratize fundraising for participants. This incident exposed critical vulnerabilities in such platforms and triggered a contentious debate on the principle of blockchain immutability. As a consequence, a network hard fork was implemented with the creation of Ethereum Classic, leading to a fundamental reassessment of the roles of hard and soft forks in blockchain governance [15].

The incident escalated when the attacker published an open letter to the Ethereum and DAO communities arguing that exploiting a systemic flaw was legal and threatening legal action against any effort to recover the funds. These actions highlighted the challenges of translating ethical norms into purely technical safeguards. Ultimately, the community abandoned the soft fork due to these newly discovered vulnerabilities and adopted a hard fork instead. The resulting split into Ethereum (ETH) and Ethereum Classic (ETC) not only resolved the immediate crisis but also stimulated a wider debate about censorship resistance and the principle of blockchain immutability [16].

The breadth of the economic questions raised by blockchain becomes particularly evident in contexts of asymmetric information. Several studies underscore the considerable room for investigation and theoretical development that remains within this emerging area of research [17]. Moreover, several studies highlight the divergence between assumptions made by computer science and economic theories concerning individual behavior [18]. Game-theoretic approaches typically assume fully rational agents, while traditional computer-science frameworks distinguish between processes that follow the prescribed protocol and Byzantine processes that deviate from it, thereby offering a more nuanced, yet still rule-based, view of behavior [18].

An illustrative case of behavioral complexity is Dogecoin, a cryptocurrency created in 2013 as a parody. Defying the rational predictions posited by game theory, Dogecoin has nevertheless achieved substantial popularity and market capitalization despite its satirical origins [19]. From an economic standpoint, the presence of cryptocurrencies like Dogecoin underscores the influence of psychological and social factors on market valuation. This example demonstrates that economic analysis of blockchain phenomena cannot disregard human behavioral dynamics, which add further complexity to the relationship between information technology and economics in this emerging field.

Recognizing this complexity, the following section reviews how previous research has addressed the interplay among incentives, behavior, and governance in blockchain systems from both economic and computer-science perspectives.

3. Overview of Previous Work

Numerous authors have explored the effect of an economic perspective on blockchain technology [20], but their discussion has mainly focused on the cryptocurrency field. Non-cryptocurrency blockchains differ substantially in the design of their monetary incentives and are frequently implemented as permissioned systems, since fully public blockchains can be unsuitable for corporate or administrative use [21]. This divergence raises important questions about how incentive structures developed for cryptocurrencies can be adapted to alternative settings.

In blockchain ecosystems, incentive structures are pivotal in encouraging miners to engage in validation activities, thereby ensuring the ongoing operation and stability of

the network. Although such mechanisms have proven effective in cryptocurrency contexts, adapting them to non-cryptocurrency applications presents a considerable challenge. Insufficient or poorly aligned incentives can therefore hinder the broader adoption of blockchain technology.

The concept of incentive compatibility, which ensures that no participant finds it advantageous to break the rules [22], is particularly relevant in this context. Within the blockchain context, incentive mechanisms are designed to ensure that the consensus protocol motivates validators to act honestly and cooperatively, complying with established rules and supporting the network's security and stability. Such incentives can include crypto rewards and penalties, as well as reputational incentives, including trust-based ratings or sanctions for deviations from expected behavior. The incentive-compatible mechanisms that operate successfully in cryptocurrency blockchains, however, are not easily transferable to non-cryptocurrency applications [9]. This requirement is particularly evident in blockchain applications that employ voting-based consensus algorithms. The existing research on this topic remains limited and predominantly focuses on designing incentive mechanisms for cryptocurrency systems that rely on proof-based consensus models [9].

It is, therefore, crucial to recognize that analyses of incentive compatibility developed for Proof-of-Work (PoW) systems cannot be directly applied to Practical Byzantine Fault Tolerance (PBFT)-based blockchains, given the fundamental differences between proof-based and voting-based consensus mechanisms. Overcoming this divide is vital for effectively integrating blockchain technology into non-cryptocurrency applications. The effectiveness of any consensus mechanism ultimately depends on the strategic behavior of the participating entities [23].

Voting-based consensus is also used in some permissionless cryptocurrency blockchains, where the large number of unidentified nodes allows for probabilistic consensus. Within this setting, rapid probabilistic consensus protocols [24,25] can lower communication costs without incurring PoW energy costs [26]. Nevertheless, to preserve network consistency and security, nodes must adhere strictly to protocol rules. The inclusion of the term "Byzantine" reflects the recognition that some nodes may act maliciously or fail to comply with the protocol. This concept is derived from the well-known Byzantine Generals Problem [27], a theoretical framework that describes the coordination problem that arises when erroneous information or malicious behavior occurs. To ensure the security and integrity of the system, a consensus algorithm is needed to prevent such malicious behavior.

Identity management and voting further illustrate these challenges [28]. Secure blockchain-based voting frameworks combine immutable identity records with cryptographic methods, such as zero-knowledge proofs and homomorphic encryption, to guarantee both voter anonymity and ballot integrity [29,30]. Digital identities are stored on-chain and governed by smart contracts that specify the creation and update rules, including possible verification by trusted authorities [31]. The voting process is regulated through smart contracts, and cryptography ensures the anonymity of votes. Smart contracts regulate the addition of new identities to the registry through a majority rule [32]. New identities are added through majority approval or other anti-Sybil mechanisms [33].

Approaches to malicious behavior differ markedly among disciplines. Computer science generally classifies nodes as either honest or faulty and analyzes protocols that remain secure as long as the percentage of faulty nodes stays below a critical threshold. Economics, by contrast, focuses on agents' utility functions and equilibrium strategies, yielding a richer account of strategic behavior. Game theory can be indispensable in addressing the self-interested nature of participants by suggesting how the incentive design may efficiently persuade participants to behave proactively [34]. Designing blockchain incentives through a game-theoretic lens is essential for motivating rational, self-interested

participants and improving network performance [35]. While game theory has proven effective in many blockchain studies, its application to PBFT is limited.

The existing studies on PBFT incentive compatibility illustrate both the progress in the field and the persistent gaps. For example, the SmartCast framework [36] introduces an off-chain incentive mechanism to address such issues, yet its effectiveness diminishes in public peer-to-peer environments, as illustrated by certain Internet of Things (IoT) applications [37]. Solidus [38] proposes a PoW-based PBFT algorithm that improves incentive compatibility but remains tied to PoW proposer selection, restricting its relevance to cryptocurrency contexts. Similarly, Wei et al. (2020) present a game-theoretic approach that concentrates on business-model incentives but offers only limited insight into the operational complexities of sustaining blockchain networks [39]. In parallel, researchers have enhanced PBFT consensus with reputation-based techniques [40,41]. While these methods improve validator selection efficiency, they do not directly resolve the fundamental incentive-compatibility problems of PBFT-based blockchains.

Taken together, these contributions underscore both the theoretical and practical importance of incentive design for non-cryptocurrency blockchains. They also reveal significant research gaps, particularly the need for integrated frameworks that reconcile consensus efficiency with robust incentive compatibility in PBFT-based architecture.

4. Reward Schemes for Vote-Based Consensus Blockchains

The broadcast process is a core element of blockchain technology. This implies the emergence of potential asymmetric information, as nodes possess private information about the content of each message they receive. The message may take a binary form, such as the retrieve/attack signal described in the Byzantine problem [27].

When coming to a non-crypto blockchain, the binary choice may be a true/false alternative. Consider the use of non-cryptocurrency blockchains for certifying competencies, property rights, or other individual characteristics. Agents acting as faulty or malicious nodes may obtain private gains by certifying false information. Consequently, the malicious agent may be externally incentivized to certify features that are not true and to broadcast messages that differ from the ones received. This is an opportunist behavior, adopted by a self-interested validator. In contrast, the honest node always broadcasts the message received. In what follows, it will be assumed that honest and malicious nodes (agents) have different utility functions. Different incentive compatibility constraints and the dominant strategies (when they exist) for each type of agent will be consequently derived. The objective is to show how an optimal reward scheme can be designed. This could be a prominent feature to ensure a reliable application of blockchain technologies for commercial, institutional, and industrial uses.

4.1. Theoretical Model

The base model considers a blockchain with $n = 3k + 1$ validators. The PBFT protocol assumes that a block is accepted if at least $2k + 1$ validators agree on its acceptance. Each validator i agrees upon the block acceptance through a v_i vote ($i = 1, \dots, n$), which can take two values:

$$v_i = \begin{cases} 1 & \text{agreement} \\ 0 & \text{rejection} \end{cases} \quad (1)$$

The block is accepted if $\sum_{i=1}^n v_i > \frac{2}{3}n$. The block is rejected if $\sum_{i=1}^n v_i \leq \frac{2}{3}n$.

This scenario is a simple representation of a PBFT protocol, where validators receive a block proposal message $M = (x, y)$, where x is the content and y is the result of the voting process on the message. In detail:

$$x = \begin{cases} 1 & \text{if the message is true} \\ 0 & \text{if the message is false} \end{cases} \quad (2)$$

$$y = \begin{cases} 1 & \text{if the message is approved} \\ 0 & \text{if the message is not approved} \end{cases} \quad (3)$$

In the blockchain validation process, validators may receive a positive reward ($w_i > 0$). The following behavioral hypotheses will be adopted:

H1. Validators can read the message and comprehend whether it is either valid or invalid.

H2. Honest validators gain increasing utility from the acceptance of valid blocks and the rejection of false blocks (with the same satisfaction gain). Faulty validators gain increasing utility from the acceptance of invalid blocks and the rejection of valid blocks (with the same satisfaction gain).

H3. Both types of validators have increasing utility in positive w_i .

The utility functions of the faulty (F) and honest (H) agents, as $U_{H,F} = f(M, w_i)$ can be accordingly described in their functional forms.

$$U'_{HM} = \frac{\partial U_H}{\partial M} \begin{cases} > 0 \text{ if } M = \begin{cases} (1,1) & \text{a true message is approved} \\ (0,0) & \text{a false message is not approved} \end{cases} \\ = 0 & \text{otherwise} \end{cases} \quad (4)$$

$$U'_{FM} = \frac{\partial U_F}{\partial M} \begin{cases} > 0 \text{ if } M = \begin{cases} (1,0) & \text{a true message is not approved} \\ (0,1) & \text{a false message is approved} \end{cases} \\ = 0 & \text{otherwise} \end{cases} \quad (5)$$

Accordingly, honest validators gain increasing utility both from the acceptance of valid blocks and from the rejection of false ones. This represents the intrinsic satisfaction derived from contributing to the proper functioning of the blockchain or the involvement in community [41]. Faulty validators, by contrast, aim to accept invalid blocks and reject valid ones (H2); their intrinsic satisfaction is thus associated with the attempt to disrupt the system. In both cases, utility also increases with the extrinsic reward (H3).

$$U'_{Hw} = \frac{\partial U_H}{\partial w} > 0 \quad (6)$$

$$U'_{Fw} = \frac{\partial U_F}{\partial w} > 0 \quad (7)$$

To simplify the notations without losing generality, let $a = U'_{HM}/U'_{Hw}$ denote the ratio between intrinsic and extrinsic marginal satisfaction for honest nodes, and let $b = U'_{FM}/U'_{Fw}$ represent the corresponding ratio for faulty nodes.

Based on these behavioral assumptions, the analysis will compare two remuneration schemes to verify the final payoffs for both types of validators. The two schemes can be summarized as follows:

Scheme A. If the vote is $v_i = 1$ and the block is accepted, the validator receives a positive w_i . If the vote is $v_i = 0$, no reward is provided.

Scheme B. If the vote is $v_i = 1$ and the block is accepted, the validator receives a positive w_i . If the vote is $v_i = 0$, and the block is rejected, the validator receives a positive w_i .

The difference between the two schemes lies in the treatment of rejection votes, which becomes critical in aligning individual incentives with collective objectives. By comparing payoffs (see Tables A1–A4 in the Appendix A), it emerges that, in Scheme A, the agreement vote ($v_i = 1$) is a dominant strategy for both honest and faulty nodes since only validators who agree on the block are rewarded. In Scheme B, no dominant strategy emerges for either type of node.

Nevertheless, payoffs depend on the voting outcome. Validators make their choices based on whether the message content is valid or invalid, without knowing if it will ultimately be accepted. The final payoffs must be expressed as expected value, conditional on the probability of block acceptance or rejection.

To compute the expected results y^e , we assume expectations follow on the PBFT distribution between honest and faulty nodes. Recalling that the PBFT protocol assumes that $2k + 1$ validators are honest, the probability of block acceptance/rejection follows Equations (8) and (9).

$$\pi(1, 1) = \pi(0, 0) = \frac{2}{3}n + 1 \quad (8)$$

$$\pi(1, 0) = \pi(0, 1) = \frac{1}{3}n - 1 \quad (9)$$

Using these probabilities, the expected payoffs for the honest (EV_H) and faulty (EV_F) nodes in Scheme A can be computed (see Equations (A1)–(A4) in the Appendix A).

By comparing the expected payoffs, it emerges that, for honest validators, $v_i = 1$ is a dominant strategy when facing valid blocks. Conversely, for false blocks, $v_i = 0$ becomes dominant only if $a > \frac{1}{3}n$. In this framework, rejection of false blocks depends on the validator's preference for honest behavior and on the network size. The balance between intrinsic and extrinsic satisfaction is crucial in determining dominant strategies.

For faulty nodes, $v_i = 1$ is a dominant strategy for false blocks, while, for valid block they vote $v_i = 0$ if $b > \frac{2}{3}n + 2$. Hence, even malicious behavior is influenced by the relative strength of intrinsic versus extrinsic satisfaction.

The expected payoffs for Scheme B are displayed in Equations (A5)–(A8) in the Appendix A. This scheme awards both positive votes for accepted blocks and negative votes for rejected blocks. For honest nodes, $v_i = 1$ is a dominant strategy with valid blocks and $v_i = 0$ with false ones. Faulty nodes vote 0 for a valid block if $a > \frac{1}{3}n + 3$ and $v_i = 1$ for false block if the same condition holds.

The honest validator is incentivized to behave correctly, as they will agree on the valid blocks and reject the false ones. On the other hand, the faulty nodes will be incentivized to behave maliciously only if their motivation is strong enough: that is, if $b > \frac{1}{3}n + 3$.

Schemes A and B are compared in Table 1, where the dominant strategies for each type of validator are displayed. Scheme B offers stronger incentives and is incentive-compatible for honest nodes, who have as dominant strategies both to accept valid blocks and reject false blocks. Scheme A is less reliable as it depends heavily on the intrinsic motivation of honest validators. At the same time, faulty nodes have a conditional dominant strategy under Scheme B for false blocks, which does not occur under Scheme A. The inclusion of extrinsic rewards in Scheme B reinforces the blockchain resistance to dishonest validation behavior.

Table 1. Dominant strategies in Schemes A and B.

	True Blocks	False Blocks
Scheme A		
Honest nodes	$V = 1$	$V = 0$ if $a > \frac{1}{3}n$
Faulty nodes	$V = 0$ if $b > \frac{2}{3}n + 2$	$V = 1$
Scheme B		
Honest nodes	$V = 1$	$V = 0$
Faulty nodes	$V = 0$ if $b > \frac{1}{3}n + 3$	$V = 1$ if $b > \frac{1}{3}n + 3$

4.2. Simulation Results

To assess the effectiveness of the proposed incentive schemes, some simulations were conducted under two main scenarios, defined by the relative weights of the coefficients a and b , and across four blockchain network sizes ($n = 12, 120, 1200$, and $12,000$).

In the first scenario, the validators derive stronger intrinsic satisfaction from adhering to their individual objectives than from the extrinsic reward (labeled ‘Strong intrinsic satisfaction’ in Tables 2 and 3). The second scenario assumes the opposite condition, where extrinsic satisfaction dominates (‘Weak intrinsic satisfaction’ in Tables 2 and 3).

Table 2. Simulation results with two thirds honest nodes.

	Scheme A				Scheme B			
	True block approvals							
	N = 12	N = 120	N = 1200	N = 12,000	N = 12	N = 120	N = 1200	N = 12,000
Strong Intrinsic Satisfaction	✓	✓	✓	✓	✓	✓	✓	✓
Votes (%)	75	67.5	66.75	66.67	75	67.5	66.75	66.67
Weak Intrinsic Satisfaction	✓	✓	✓	✓	✓	✓	✓	✓
Votes (%)	100	100	100	100	100	100	100	100
	False block approvals							
Strong Intrinsic Satisfaction	✗	✗	✗	✗	✗	✗	✗	✗
Votes (%)	25	32.5	33.25	33.32	25	32.5	33.25	33.32
Weak Intrinsic Satisfaction	✓	✓	✓	✓	✗	✗	✗	✗
Votes (%)	100	100	100	100	25	32.5	33.25	33.32

Table 3. Simulation results with one-half-plus-one honest nodes.

	Scheme A				Scheme B			
	True block approvals							
	<i>n</i> = 12	<i>n</i> = 120	<i>n</i> = 1200	<i>n</i> = 12,000	<i>n</i> = 12	<i>n</i> = 120	<i>n</i> = 1200	<i>n</i> = 12,000
Strong Intrinsic Satisfaction	✓	✓	✓	✓	✓	✓	✓	✓
Votes (%)	75	67.5	66.75	66.67	58.33	50.83	50.08	50.01
Weak Intrinsic Satisfaction	✓	✓	✓	✓	✓	✓	✓	✓
Votes (%)	100	100	100	100	100	100	100	100
	False blocks approvals							
Strong Intrinsic Satisfaction	✗	✗	✗	✗	✗	✗	✗	✗
Votes (%)	25	32.5	33.25	33.32	41.66	49.16	49.91	49.99
Weak Intrinsic Satisfaction	✓	✓	✓	✓	✗	✗	✗	✗
Votes (%)	100	100	100	100	41.66	49.16	49.91	49.99

Additionally, two different voter compositions were tested. Table 2 presents results assuming that two thirds of nodes are honest; Table 3 considers a simple majority (one half plus one) of honest voters. For each configuration, the percentage of approval votes was recorded both for true and false blocks.

Comparing the results of Scheme A and Scheme B, both schemes clearly perform robustly when approving true blocks. When false blocks are proposed, however, Scheme A tends to approve them, whereas Scheme B consistently rejects them.

These outcomes highlight the greater robustness and reliability of Scheme B, particularly in maintaining consensus integrity against dishonest behaviors and suggest that the design of the reward mechanism plays a decisive role in sustaining the integrity and efficiency of decentralized systems. By ensuring that honest behavior is both individually rational and collectively beneficial, Scheme B provides a more sustainable equilibrium between autonomy and accountability within blockchain-based organizations. Moreover, the observed stability of the results across different network dimensions implies scalability, making the incentive structure potentially applicable to both small and large decentralized organizations, such as DAOs.

5. Incentives and Governance Challenges in Decentralized Autonomous Organizations

This section examines how blockchain-based incentive mechanisms can strengthen Decentralized Autonomous Organizations (DAOs) and, more broadly, decentralized governance. Building on the previous analysis of incentive compatibility, it considers DAOs not only as technological innovations but also as new forms of economic organization.

DAOs are blockchain-driven organizations that allow participants to coordinate and govern themselves through self-executing smart contracts, with decision-making distributed across the network [42]. The study of decentralized organizational models has a long history in organizational theory, with significant discussions emerging as early as the mid-20th century [43,44]. The rise in peer-to-peer economies underscores the need for adaptive organizational models that mirror the dynamics of complex systems, where collective output exceeds the sum of individual members' contributions [45]. The discussion on DAOs has evolved over time, from early applications in multi-agent systems and IoT networks [46] to contemporary blockchain-based implementations. Some scholars even view Bitcoin as the first DAO [47].

Vitalik Buterin, in the Ethereum white paper, described a DAO as a “virtual entity” that allows members or shareholders to manage funds and governance purely through blockchain-based systems [48]. This approach aims to replicate the operational and governance frameworks of traditional companies or nonprofits but with enforcement achieved through cryptography rather than legal institutions [49].

Ethereum played a pivotal role in the DAO ecosystem, notably with *The DAO* in 2016 [50], a venture-capital project that attracted significant attention despite its failure, which was primarily due to a vulnerability known as the Reentrancy Attack, which occurs when an attacker drains funds from a target contract by recursively calling its withdrawal function before the initial execution is complete. This oversight allows the attacker to repeatedly invoke the withdrawal function, effectively draining the contract's funds. In the case of the DAO, the attacker exploited this vulnerability to siphon approximately 3.6 million Ether, valued at around 50 million U.S. dollars at the time [51]. The vulnerability lies in the victim's contract failing to update the balance of the malicious actor before transferring the funds, allowing the attacker to re-enter the withdrawal process and drain more Ether than the number to which they were entitled [52].

This incident highlights a critical oversight in the development and auditing processes of smart contracts. Despite this significant setback, the DAO's experiment paved the way for the development of other DAOs, such as MolochDAO and MetaCartel. It led to the creation of platforms that support DAOs, such as Aragon and DAOstack. Colony is a blockchain-based DAO for labor-managed firms [53]. These DAOs have inspired related models, such as the Decentralized Collaborative Organization (DCO), which emphasizes collaboration among participants [54].

DAOs are recognized for enabling online coordination and self-management and maintaining governance that is independent of any central authority [54,55]. Although the academic study of DAOs is still in its early stages, a growing body of research focuses on blockchain's role in new business models, such as decentralized exchanges [56] and prediction markets [57]. DAOs offer flexibility, enabling the creation of diverse entities, from crowdfunding platforms to fully automated companies and decision-making systems.

Governance within DAOs has become a key area of research. Some studies have examined how blockchain and smart contracts can facilitate new decentralized governance models [58,59]. Questions surrounding accountability and regulatory challenges remain significant obstacles, however [50,60–62]. While DAOs are seen as tools for economic and political decentralization [63], questions persist regarding autonomy, human oversight, and legal recognition [64,65]. The question of DAO legal personhood is especially challenging, since autonomous smart contracts lack the identifiable actors required for legal liability.

Aligning individual incentives with collective objectives remains a fundamental challenge for DAOs. Traditional command structures often fail to adapt to the decentralized nature of DAOs, whereas blockchain-based smart contracts can formalize governance rules and maintain transparent, immutable records of participation. By incentivizing participation through blockchain-based rewards, organizations can foster decentralized governance structures that combine autonomy with accountability. The extension of blockchain-based incentive models to DAOs represents a significant opportunity for businesses to decentralize authority and to scale efficiently without sacrificing individual autonomy, without the bottlenecks of resource constraints or centralized decision-making. Additionally, this decentralized approach reduces the risks associated with central points of failure, enhancing an organization's overall resilience and adaptability.

As summarized in Figure 1, sustainable governance in blockchain-based organizations emerges from the interaction among validator preferences, incentive mechanisms, and consensus outcomes. This integrated framework emphasizes that the design of reward structures has cascading effects on organizational performance and the broader sustainability of the system.

The interaction depicted in Figure 1 reveals how economic incentives translate into governance outcomes within decentralized systems. By influencing validator behavior, reward structures determine whether a DAO achieves sustainable coordination or degenerates into opportunistic dynamics. In this sense, incentive design acts as an institutional substitute for traditional hierarchies, providing order and predictability in otherwise self-organizing systems. This perspective highlights that the sustainability of DAOs ultimately rests on the alignment of economic rationality with collective governance goals.

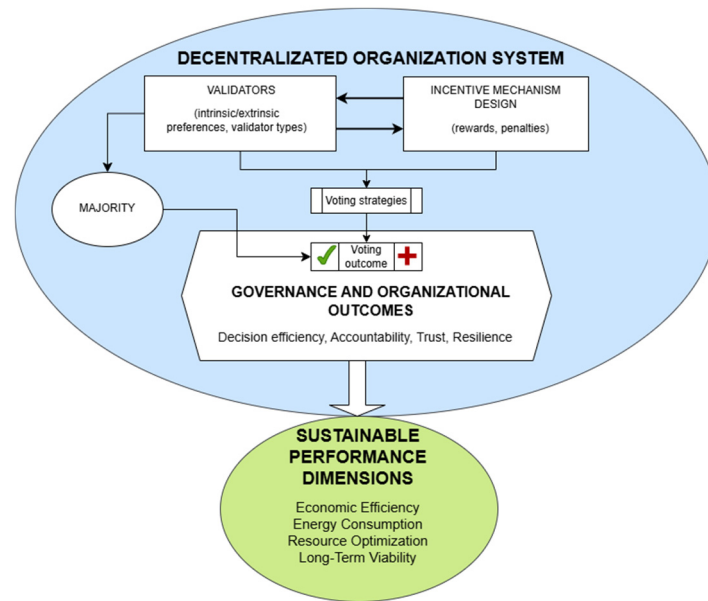


Figure 1. Relationship among incentive mechanism design, validator behavior, and governance outcomes in decentralized organizations.

6. Conclusions

The objective of this study was to show that applications of blockchain technology enable a more accurate evaluation of the individual behaviors of agents participating in the network. Viewing nodes as economic actors enables a more precise understanding of how incentive mechanisms and consensus protocols shape behavior. At the same time, the deployment of blockchain technologies must also be assessed in terms of their long-term economic viability and environmental sustainability. The design of incentive mechanisms and consensus protocols must not only align with agents' strategic behavior but also ensure that the system operates with acceptable energy consumption and resource efficiency.

Using a game-theoretic approach, this study analyzed typical challenges of voting-based consensus mechanisms by comparing two alternative reward schemes to show how mechanism design influences adherence to protocol rules. Furthermore, the incentive compatibility problem of voting-based consensus mechanisms was compared with some case studies specifically concerning DAOs. These organizations represent a significant opportunity for businesses and communities to decentralize authority, enhance member engagement, and ensure operational efficiency through structured and equitable reward systems. By implementing smart contracts and blockchain-based incentives, DAOs can overcome traditional organizational challenges related to accountability and scalability.

Future research should further investigate how DAOs and other decentralized governance models can integrate sustainability criteria directly into their design. Embedding energy efficiency, fair resource allocation, and long-term resilience into smart contracts and incentive schemes will be key to ensuring that decentralized systems contribute positively to both economic development and environmental stewardship.

The limitations of the present study lie in its inherently static framework. A dynamic perspective would provide a more realistic representation of cooperative behavior. In repeated games, the "grim trigger strategy" serves as a mechanism to encourage cooperation among players [66,67]. The dynamic perspective is crucial not only to reinforce cooperative behavior [68] but also for sustainability: inefficient consensus models that encourage short-term opportunistic behavior or consume excessive computational resources may undermine both the economic and ecological feasibility of blockchain adoption. Incorporating adaptive, reputation-based mechanisms reduces wasted effort and energy while

reinforcing cooperative dynamics. Further research could also clarify how a more nuanced classification of agent behaviors could enrich the analysis. Moreover, the present work focuses on conceptual and simulation-based analysis, but a quantitative assessment of energy efficiency or economic cost metrics remains an open area for future investigation, pending the availability of robust empirical data.

In conclusion, this study highlights the pivotal role of incentive mechanisms in shaping participant behavior and ensuring network integrity of blockchain networks. By applying game theory, we demonstrated how strategic interactions within these networks can be optimized to promote cooperation and discourage malicious activities. Ethical and legal considerations remain central to the broader adoption of blockchain technologies. Overall, the findings suggest that blockchain and DAOs hold significant potential to transform economic and governance structures by balancing autonomy with accountability and leveraging transparency and security to achieve sustainable and resilient organizational models. The ongoing research and development in this field will be central to addressing the remaining challenges and fully realizing the potential of decentralized organizations.

Author Contributions: Conceptualization, B.B., A.M. and V.V.; Formal analysis, B.B.; Investigation, A.M.; Writing—original draft, A.M.; Writing—review and editing, B.B. and A.M.; Supervision, B.B. and V.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article material. Further inquiries can be directed to the corresponding author.

Acknowledgments: This article is an expanded version of a paper [10], which was presented at the Distributed Ledger Technology Workshop 2024, the Sixth Distributed Ledger Technology Workshop (DLT 2024), Turin, Italy, 14–15 May 2024.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Final payoffs—Scheme A—honest nodes.

Strategies	Messages			
	$M = (1, 1)$	$M = (1, 0)$	$M = (0, 0)$	$M = (0, 1)$
$v_i = 1$	$(a + 1)U'_{H_w}$		aU'_{H_w}	U'_{H_w}
$v_i = 0$	aU'_{H_w}		aU'_{H_w}	

Table A2. Final payoffs—Scheme A—faulty nodes.

Strategies	Messages			
	$M = (1, 1)$	$M = (1, 0)$	$M = (0, 0)$	$M = (0, 1)$
$v_i = 1$	U'_{F_w}	bU'_{F_w}		$(b + 1)U'_{F_w}$
$v_i = 0$		bU'_{F_w}		bU'_{F_w}

Table A3. Final payoffs—Scheme B—honest nodes.

Strategies	Messages			
	$M = (1, 1)$	$M = (1, 0)$	$M = (0, 0)$	$M = (0, 1)$
$v_i = 1$	$(a + 1)U'_{H_w}$		aU'_{H_w}	U'_{H_w}
$v_i = 0$	aU'_{H_w}	U'_{H_w}	$(a + 1)U'_{H_w}$	

Table A4. Final payoffs—Scheme B—faulty nodes.

Strategies	Messages			
	$M = (1, 1)$	$M = (1, 0)$	$M = (0, 0)$	$M = (0, 1)$
$v_i = 1$	U'_{F_w}	bU'_{F_w}		$(b + 1)U'_{F_w}$
$v_i = 0$		$(b + 1)U'_{F_w}$	U'_{F_w}	bU'_{F_w}

$$EVH(1, ye) = \begin{cases} (\frac{2}{3}n + 1)(a + 1)U'_{H_w} & \text{if } v_i = 1 \\ (\frac{2}{3}n)aU'_{H_w} & \text{if } v_i = 0 \end{cases} \quad (A1)$$

$$EVH(0, ye) = \begin{cases} (\frac{2}{3}n)aU'_{H_w} + (\frac{1}{3}n)U'_{H_w} & \text{if } v_i = 1 \\ (\frac{2}{3}n + 1)aU'_{H_w} & \text{if } v_i = 0 \end{cases} \quad (A2)$$

$$EVF(1, ye) = \begin{cases} (\frac{2}{3}n + 2)U'_{F_w} + (\frac{1}{3}n - 2)bU'_{F_w} & \text{if } v_i = 1 \\ (\frac{1}{3}n - 1)bU'_{F_w} & \text{if } v_i = 0 \end{cases} \quad (A3)$$

$$EVF(0, ye) = \begin{cases} (\frac{1}{3}n - 1)(b + 1)U'_{F_w} & \text{if } v_i = 1 \\ (\frac{1}{3}n - 1 - 1)bU'_{F_w} & \text{if } v_i = 0 \end{cases} \quad (A4)$$

$$EVH(1, ye) = \begin{cases} (\frac{2}{3}n + 1)(a + 1)U'_{H_w} & \text{if } v_i = 1 \\ (\frac{2}{3}n)aU'_{H_w} + (\frac{1}{3}n)U'_{H_w} & \text{if } v_i = 0 \end{cases} \quad (A5)$$

$$EVH(0, ye) = \begin{cases} (\frac{2}{3}n)aU'_{H_w} + (\frac{1}{3}n)U'_{H_w} & \text{if } v_i = 1 \\ (\frac{2}{3}n + 1)(a + 1)U'_{H_w} & \text{if } v_i = 0 \end{cases} \quad (A6)$$

$$EVF(1, ye) = \begin{cases} (\frac{2}{3}n + 2)U'_{F_w} + (\frac{1}{3}n - 2)bU'_{F_w} & \text{if } v_i = 1 \\ (\frac{1}{3}n - 1)(b + 1)U'_{F_w} & \text{if } v_i = 0 \end{cases} \quad (A7)$$

$$EVF(0, ye) = \begin{cases} (\frac{1}{3}n - 1)(b + 1)U'_{F_w} & \text{if } v_i = 1 \\ (\frac{1}{3}n - 2)bU'_{F_w} + (\frac{2}{3}n + 2)U'_{F_w} & \text{if } v_i = 0 \end{cases} \quad (A8)$$

References

1. Nakamoto, S. A Peer-to-Peer Electronic Cash System. *Bitcoin* **2008**, *4*, 15.
2. Kane, E. Is Blockchain a General Purpose Technology? 2017. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2932585 (accessed on 29 September 2025).
3. Rodriguez Müller, A.P.; Martin Bosch, J.; Tangi, L. An Overview of the Expected Public Values Arising from Blockchain Adoption in the European Public Sector. *Int. J. Public Sect. Manag.* **2025**, *38*, 53–76. [CrossRef]
4. Abeyratne, S.; Monfared, R. Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. *Int. J. Res. Eng. Technol.* **2016**, *5*, 1–10. [CrossRef]
5. Engelhardt, M.A. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [CrossRef]

6. Jøsang, A. Identity Management and Trusted Interaction in Internet and Mobile Computing. *IET Inf. Secur.* **2014**, *8*, 67–79. [CrossRef]
7. Korpela, K.; Hallikas, J.; Dahlberg, T. Digital Supply Chain Transformation toward Blockchain Integration. In Proceedings of the 50th Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017.
8. Murano, A.; Bruno, B.; Vespri, V. Blockchain Barriers in Public Organizations: A Systematic Literature Review. *Socioecon. Plann. Sci.* **2025**, *103*, 102364. [CrossRef]
9. Li, X.; Liu, Q.; Wu, S.; Cao, Z.; Bai, Q. Game Theory Based Compatible Incentive Mechanism Design for Non-Cryptocurrency Blockchain Systems. *J. Ind. Inf. Integr.* **2023**, *31*, 100426. [CrossRef]
10. Murano, A.; Bruno, B.; Vespri, V. Incentive Compatibility in Consensus Protocols and DAOs: A Game-Theoretic Approach. In Proceedings of the Distributed Ledger Technology Workshop 2024, Proceedings of the Sixth Distributed Ledger Technology Workshop (DLT 2024), Turin, Italy, 14–15 May 2024.
11. Buchanan, J.M. The Constitution of Economic Policy. *Am. Econ. Rev.* **1987**, *77*, 243–250. [CrossRef] [PubMed]
12. Pazaitis, A.; De Filippi, P.; Kostakis, V. Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed. *Technol. Forecast. Soc. Change* **2017**, *125*, 105–115. [CrossRef]
13. Bissias, G.; Ozisik, A.P.; Levine, B.N.; Liberatore, M. Sybil-Resistant Mixing for Bitcoin. In Proceedings of the 13th Workshop on Privacy in the Electronic Society, Scottsdale, AR, USA, 3 November 2014; pp. 149–158.
14. Kamvar, S.D.; Schlosser, M.T.; Garcia-Molina, H. Incentives for Combatting Freeriding on P2P Networks. In *Euro-Par 2003 Parallel Processing*; Kosch, H., Böszörményi, L., Hellwagner, H., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2790, pp. 1273–1279, ISBN 978-3-540-40788-1.
15. Mehar, M.I.; Shier, C.L.; Giambattista, A.; Gong, E.; Fletcher, G.; Sanayhie, R.; Kim, H.M.; Laskowski, M. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. *J. Cases Inf. Technol.* **2019**, *21*, 19–32. [CrossRef]
16. Zhao, X.; Chen, Z.; Chen, X.; Wang, Y.; Tang, C. The DAO Attack Paradoxes in Propositional Logic. In Proceedings of the 2017 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, China, 11–13 November 2017; pp. 1743–1746.
17. Ante, L. A Place Next to Satoshi: Foundations of Blockchain and Cryptocurrency Research in Business and Economics. *Scientometrics* **2020**, *124*, 1305–1333. [CrossRef]
18. Amoussou-Guenou, Y.; Biais, B.; Potop-Butucaru, M.; Tucci-Piergiovanni, S. Committee-Based Blockchains as Games between Opportunistic Players and Adversaries. *Rev. Financ. Stud.* **2023**, *37*, 409–443. [CrossRef]
19. Rahman, I.A.; Indrakusuma, T.; Widodo, A.; Nuryadin, D. Dogecoin Price Volatility After Economic Recovery on COVID-19 Pandemic. *Int. J. Adv. Econ.* **2023**, *5*, 129–137. [CrossRef]
20. Chen, L.; Cong, L.W.; Xiao, Y. A Brief Introduction to Blockchain Economics. In *Information for Efficient Decision Making*; World Scientific: Singapore, 2020; pp. 1–40, ISBN 978-981-12-2046-3.
21. Dib, A.; Brousmiche, K.; Durand, A.; Thea, E.; Hamida, E.D. Consortium Blockchains: Overview, Applications and Challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64.
22. Ledyard, J.O. Incentive Compatibility. In *Allocation, Information and Markets*; Eatwell, J., Milgate, M., Newman, P., Eds.; Palgrave Macmillan: London, UK, 1989; pp. 141–151, ISBN 978-0-333-49539-1.
23. Li, T.; Chen, Y.; Wang, Y.; Wang, Y.; Zhao, M.; Zhu, H.; Tian, Y.; Yu, X.; Yang, Y. Rational Protocols and Attacks in Blockchain System. *Secur. Commun. Netw.* **2020**, *2020*, 8839047. [CrossRef]
24. Mitra, D.; Cortesi, A.; Chaki, N. A Two-Hop Neighborhood Based Berserk Detection Algorithm for Probabilistic Model of Consensus in Distributed Ledger Systems. Available online: https://link.springer.com/chapter/10.1007/978-3-031-41456-5_29 (accessed on 7 October 2024).
25. Popov, S.; Buchanan, W. FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures. *J. Parallel Distrib. Comput.* **2020**, *147*, 77–86. [CrossRef]
26. Popov, S.; Müller, S. Voting-Based Probabilistic Consensus and Their Applications in Distributed Ledgers. *Ann. Telecommun.* **2021**, *77*, 77–99. [CrossRef]
27. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* **1982**, *4*, 382401. [CrossRef]
28. Clarke, R.; McGuire, L.; Baza, M.; Rasheed, A.; Alsabaan, M. Online Voting Scheme Using IBM Cloud-Based Hyperledger Fabric with Privacy-Preservation. *Appl. Sci.* **2023**, *13*, 7905. [CrossRef]
29. Kumar, S.R.; Goyal, M. Administration of Digital Identities Using Blockchain. In Proceedings of the 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 14–16 December 2022; IEEE: Uttar Pradesh, India, 2022; pp. 2179–2183.
30. Miao, Y. Secure and Privacy-Preserving Voting System Using Zero-Knowledge Proofs. *Appl. Comput. Eng.* **2023**, *8*, 328–333. [CrossRef]
31. Gilani, K.; Ghaffari, F.; Bertin, E.; Crespi, N. Self-Sovereign Identity Management Framework using Smart Contracts. In Proceedings of the NOMS 2022—2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; IEEE: Budapest, Hungary, 2022; pp. 1–7.

32. Shermin, V. Disrupting Governance with Blockchains and Smart Contracts. *Strateg. Change* **2017**, *26*, 499–509. [CrossRef]
33. Platt, M.; McBurney, P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms* **2023**, *16*, 34. [CrossRef]
34. Wen, Y.; Lu, F.; Liu, Y.; Huang, X. Attacks and Countermeasures on Blockchains: A Survey from Layering Perspective. *Comput. Netw.* **2021**, *191*, 107978. [CrossRef]
35. Zhu, X.; Li, Y.; Fang, L.; Chen, P. An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services. *IEEE Access* **2020**, *8*, 102177–102187. [CrossRef]
36. Kothapalli, A.; Miller, A.; Borisov, N. SmartCast: An Incentive Compatible Consensus Protocol Using Smart Contracts. In *Financial Cryptography and Data Security*; Brenner, M., Rohloff, K., Bonneau, J., Miller, A., Ryan, P.Y.A., Teague, V., Bracciali, A., Sala, M., Pintore, F., Jakobsson, M., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2017; Volume 10323, pp. 536–552, ISBN 978-3-319-70277-3.
37. Lao, L.; Dai, X.; Xiao, B.; Guo, S. G-PBFT: A Location-Based and Scalable Consensus Protocol for IoT-Blockchain Applications. In Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS), New Orleans, LA, USA, 18–22 May 2020; IEEE: New Orleans, LA, USA, 2020; pp. 664–673.
38. Abraham, I.; Malkhi, D.; Nayak, K.; Ren, L.; Spiegelman, A. Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus. *arXiv* **2017**, arXiv:1612.02916. [CrossRef]
39. Wei, L.; Wu, J.; Long, C. A Blockchain-Based Hybrid Incentive Model for Crowdsensing. *Electronics* **2020**, *9*, 215. [CrossRef]
40. Lei, K.; Zhang, Q.; Xu, L.; Qi, Z. Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; IEEE: Singapore, 2018; pp. 604–611.
41. Dhillon, R.; Sivabalan, P. Exploring Dimensions of Governance for Different Types of Blockchain Systems. *Br. Account. Rev.* **2025**, 101588. [CrossRef]
42. Wright, A.; De Filippi, P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia 2015. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (accessed on 29 September 2025).
43. Freeland, J.R.; Baker, N.R. Goal Partitioning in a Hierarchical Organization. *Omega* **1975**, *3*, 673–688. [CrossRef]
44. Shubik, M. Incentives, Decentralized Control, the Assignment of Joint Costs and Internal Pricing. *Manag. Sci.* **1962**, *8*, 325–343. [CrossRef]
45. Johnson, N. *Simply Complexity: A Clear Guide to Complexity Theory*; Simon and Schuster: New York, NY, USA, 2009; ISBN 978-1-78074-049-2.
46. Dilger, W. Decentralized Autonomous Organization of the Intelligent Home According to the Principle of the Immune System. In Proceedings of the Computational Cybernetics and Simulation 1997 IEEE International Conference on Systems, Man, and Cybernetics, Orlando, FL, USA, 12–15 October 1997; Volume 1, pp. 351–356.
47. Hsieh, Y.-Y.; Vergne, J.-P.; Anderson, P.; Lakhani, K.; Reitzig, M. Bitcoin and the Rise of Decentralized Autonomous Organizations. *J. Organ. Des.* **2018**, *7*, 14. [CrossRef]
48. Buterin, V. A Next Generation Smart Contract & Decentralized Application Platform. 2014. Available online: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf (accessed on 29 September 2025).
49. De Filippi, P.; Reijers, W.; Mannan, M. *Blockchain Governance*; The MIT Press Essential Knowledge Series; The MIT Press: Cambridge, MA, USA, 2024; ISBN 978-0-262-54905-9.
50. DuPont, Q. Experiments in Algorithmic Governance | 8 | A History and Ethnography. Available online: <https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781315211909-8/experiments-algorithmic-governance-quinn-dupont> (accessed on 18 August 2024).
51. Fatima Samreen, N.; Alalfi, M.H. Reentrancy Vulnerability Identification in Ethereum Smart Contracts. In Proceedings of the 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), London, ON, Canada, 18 February 2020; pp. 22–29.
52. DASP—TOP 10. Available online: <https://dasp.co/> (accessed on 16 September 2024).
53. Mannan, M. Fostering Worker Cooperatives with Blockchain Technology: Lessons from the Colony Project. *Erasmus Law Rev.* **2018**, *11*, 190–203. [CrossRef]
54. Davidson, S.; De Filippi, P.; Potts, J. Blockchains and the Economic Institutions of Capitalism. *J. Institutional Econ.* **2018**, *14*, 639–658. [CrossRef]
55. Singh, M.; Kim, S. Chapter Four—Blockchain Technology for Decentralized Autonomous Organizations. In *Advances in Computers*; Kim, S., Deka, G.C., Zhang, P., Eds.; Role of Blockchain Technology in IoT Applications; Elsevier: Amsterdam, The Netherlands, 2019; Volume 115, pp. 115–140.
56. Lin, L.X.; Budish, E.; Cong, L.W.; He, Z.; Bergquist, J.H.; Panesir, M.S.; Kelly, J.; Lauer, M.; Prinster, R.; Zhang, S. Deconstructing Decentralized Exchanges. *Stanf. J. Blockchain Law Policy* **2019**, *2*, 58–77. Available online: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/sjblp2&div=4&id=&page=> (accessed on 18 August 2024).

57. Clark, J.; Bonneau, J.; Miller, A.; Felten, E.; Kroll, J.A.; Narayanan, A. On Decentralizing Prediction Markets and Order Books. 2014. Available online: <https://econinfosec.org/archive/weis2014/presentations/Clark-WEIS2014-Slides.pdf> (accessed on 29 September 2025).
58. Leonhard, R. Corporate Governance on Ethereum’s Blockchain. 2017. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977522 (accessed on 29 September 2025).
59. Rozas, D.; Tenorio Fornés, Á.; Díaz Molina, S.; Hassan Collado, S. When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. *Sage Open* **2021**, *11*, 21582440211002526. [CrossRef]
60. Garrod, J.Z. The Real World of the Decentralized Autonomous Society. *TripleC Commun. Capital. Crit. Open Access J. Glob. Sustain. Inf. Soc.* **2016**, *14*, 62–77. [CrossRef]
61. Scott, B.; Loonam, J.; Kumar, V. Exploring the Rise of Blockchain Technology: Towards Distributed Collaborative Organizations—Scott—2017—Strategic Change—Wiley Online Library. Available online: <https://onlinelibrary.wiley.com/doi/10.1002/jsc.2142> (accessed on 18 August 2024).
62. Anyanwu, A.; Dawodu, S.O.; Omotosho, A.; Akindote, O.J.; Ewuga, S.K. Review of Blockchain Technology in Government Systems: Applications and Impacts in the USA. *World J. Adv. Res. Rev.* **2023**, *20*, 863–875. [CrossRef]
63. Atzori, M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? 2015. Available online: <https://ssrn.com/abstract=2709713> (accessed on 29 October 2025).
64. Beck, R. Beyond Bitcoin: The Rise of Blockchain World. *Computer* **2018**, *51*, 54–58. [CrossRef]
65. Davidson, S.; De Filippi, P.; Potts, J. Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. 2016. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995 (accessed on 29 September 2025).
66. Fan, C.-P. Teaching Children Cooperation—An Application of Experimental Game Theory. *J. Econ. Behav. Organ.* **2000**, *41*, 191–209. [CrossRef]
67. Axelrod, R.M. *The Evolution of Cooperation*; Basic Books: New York, NY, USA, 1984; ISBN 978-0-465-02121-5.
68. Dixit, A.K.; Skeath, S.; McAdams, D. *Games of Strategy*, 5th ed.; International Student Edition, Not for Sale in the United States or Canada; W. W. Norton & Company: New York, NY, USA, 2021; ISBN 978-0-393-42220-7.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.