



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

in cotutela con University of Luxembourg - Université du Luxembourg

DOTTORATO DI RICERCA IN
LAW, SCIENCE AND TECHNOLOGY

Ciclo 38

Settore Concorsuale: 12/H3 - FILOSOFIA DEL DIRITTO

Settore Scientifico Disciplinare: IUS/20 - FILOSOFIA DEL DIRITTO

BLOCKCHAIN TECHNOLOGY, GOVERNANCE AND LAW: TAMING THE
ALGORITHMIC LEVIATHAN

Presentata da: Ali Mert Gurkan

Coordinatore Dottorato

Antonino Rotolo

Supervisore

Monica Palmirani

Co-supervisore

CHRISTOPH SCHOMMER

Esame finale anno 2026



PhD-FSTM-2026-024

Faculty of Science, Technology and Medicine

DOCTORATE IN LAW, SCIENCE, AND
TECHNOLOGY – LAST- JD Cycle
XXXVIII

DISSERTATION

Defence held on 13 April 2026 in Bologna

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

AND

DOCTEUR DE L'UNIVERSITÉ Du BOLOGNA

EN DROIT, SCIENCE ET TECHNOLOGIE

by

Gürkan ALİ MERT

Born on 24 April 1995 in Seyhan (Türkiye)

Blockchain Technology, Governance and Law:
Taming the Algorithmic Leviathan

Dissertation defence committee

Prof. Dr Christoph SCHOMMER, Supervisor

Associate professor in Artificial Intelligence, UNIVERSITÉ DU LUXEMBOURG / Esch-sur-Alzette / Luxembourg

Prof. Dr Monica PALMIRANI, Co-Supervisor

UNIVERSITY OF BOLOGNA / Bologna BO / Italy

Prof. Dr Cristina PONCIBÒ, Chair

Full Professor, UNIVERSITÀ DI TORINO / Torino / Italy

Mr/Ms Filippo ZATTI, Member

Associate Professor, UNIVERSITY OF FLORENCE / Florence / Italy

Prof. Dr Francesca SPIGARELLI, Member

Full Professor, UNIVERSITA DI MACERATA / Macerata / Italy

Abstract

This thesis investigates the profound conceptual and practical challenges arising from the integration of blockchain technology, rooted in an ideology of radical decentralization, into established, centralized frameworks of public and corporate governance. Conceived by cypherpunk movements as a means to replace fallible human intermediaries with the cryptographic certainty of "Code is Law," blockchain promises trustless, automated coordination. However, this research argues that the technology's revolutionary potential has been decisively neutralized by the normative and structural power of existing legal and institutional orders. Rather than disrupting governance, blockchain is undergoing cautious institutional adaptation and pragmatic co-option, demonstrating the enduring supremacy of the rule of law over algorithmic absolutism.

The analysis unfolds across four chapters, tracing blockchain's journey from ideological origin to institutional encounter. *Chapter 1* establishes blockchain's political genesis as a response to perceived failures of state and corporate power, aiming to create self-sovereign systems via *Lex Cryptographia*. *Chapter 2* tests this vision against the constitutional state, identifying a fundamental "Governance Paradox." Blockchain's core features, immutability and decentralization, clash irreconcilably with public law's requirements for discretion, correctability (e.g., GDPR's right to erasure), and hierarchical accountability. Consequently, states universally prefer permissioned blockchains, domesticating the technology to reinforce, not replace, state authority, primarily for enhancing data integrity and inter-agency coordination.

Chapter 3 examines Decentralized Autonomous Organizations (DAOs) as the purest private-sector experiment in "Code is Law" governance. It finds this experiment largely fails on its own terms, succumbing to governance pathologies like plutocratic capture by wealthy "whales" and the emergence of unaccountable technocratic elites among core developers. The infamous 2016 hack of "The DAO" demonstrated the model's brittleness and the ultimate sovereignty of off-chain human consensus over immutable code.

Chapter 4 provides the legal reckoning, revealing DAOs as a catastrophic "Legal Misfit" under corporate law. Lacking legal personality and limited liability, native DAOs default to general partnerships, exposing participants to unlimited personal liability, as confirmed in landmark cases like *CFTC v. Ooki DAO*. DAOs fail to replicate essential corporate safeguards like fiduciary duties, leaving governance vulnerable.

Drawing from law, political philosophy, and organizational studies, this thesis introduces new ways to understand blockchain's challenges, specifically through the concepts of the "Governance Paradox" and the "Legal Misfit". It serves as a sober corrective to techno-utopianism, highlighting severe risks like unlimited liability and plutocratic capture. The findings underscore the urgent need for legal clarity, including bespoke legal forms for DAOs offering limited liability, alongside problem-driven, legally-grounded approaches for public sector adoption. Ultimately, the successful integration of blockchain hinges not on its technical elegance, but on its clear subordination to and careful integration within the enduring principles of human-centric law and democratic accountability.

Table of Contents

Table of Contents.....	3
1 Introduction.....	7
1.1 Notes on Methodology.....	8
1.2 Structure of the Thesis / Outlook.....	9
2 Chapter 1: The Ideological History of the Blockchain Technology: From Cyberspace to Bitcoin.....	12
2.1 Introduction and Research Context	12
2.1.1 Research Statement and Questions	13
2.1.2 Methodological Framework	13
2.1.3 Contributions.....	14
2.1.4 Literature Review.....	15
2.1.5 Chapter Structure and Plan.....	16
2.2 Setting the Stage: The History of Blockchain Before Blockchain.....	17
2.2.1 Early Visions of a Decentralized Cyberspace	18
2.2.2 The Californian Ideology	19
2.2.3 The Enclosure of the Digital Commons.....	19
2.2.4 Network Effects and Winner-Takes-All Dynamics.....	20
2.2.5 Platforms, Privatization, and Governance by Code	21
2.2.6 The Democratic and Societal Implications	21
2.2.7 Code is Law.....	22
2.2.8 Rule by Code.....	23
2.3 The Cypherpunk Counter-Revolution	24
2.3.1 Origins, Ethos, and the Mailing List	24
2.3.2 The Foundational Manifestos.....	25
2.3.3 The Crypto Wars and Resistance to State Control	25
2.3.4 The Search for Digital Cash	26
2.4 The Nakamoto Synthesis: The Invention of Blockchain.....	28
2.4.1 Bitcoin as a Response to Financial Crisis and Distrust.....	28
2.4.2 Weaving the Threads.....	29
2.4.3 Defining Blockchain as a New Architecture of Trust	29
2.4.4 Blockchain as a Synthesis of Philosophy, Economics, and Code	30
2.5 The Technical Apparatus of a Trust Machine.....	32
2.5.1 The Data Structure: Blocks, Hashes, and the Chain	33
2.5.2 Cryptographic Sovereignty: Keys, Wallets, and Ownership.....	33
2.5.3 The Peer-to-Peer Architecture: Resilience and Propagation	34
2.5.4 The Consensus Mechanism: Forging Agreement in a Distributed System	35
2.6 A Critical Analysis	36
2.7 Conclusion: From Ideology to Infrastructure	38
3 Chapter 2: Blockchain in Public Governance	39
3.1 Introduction and Research Context	39
3.1.1 Research Statement and Questions	39
3.1.2 Methodology	40
3.1.3 Research Design and Approach	40

3.1.4	Contributions.....	42
3.1.5	Literature Review.....	42
3.1.6	Chapter Structure and Plan.....	44
3.2	Public Governance as a Normative Constitutional Framework.....	47
3.2.1	A Power Shift	49
3.2.2	The Central Tension: Reconciling Blockchain with Constitutional Law	50
3.3	Blockchain and New Public Governance	52
3.3.1	From Bureaucracy to Networks: Setting the Context	52
3.3.2	The Emergence of New Public Governance	53
3.3.3	Blockchain and NPG: Conceptual Convergence	54
3.4	Blockchain as an Enabler of Collaborative Public Value	54
3.4.1	Institutional Adaptation and the Algorithmic State	55
3.4.2	From Theory to Translation	55
3.5	The Technical Properties of Blockchain in the Governmental Design	56
3.5.1	Data Protection as a Hard Constraint on Blockchain.....	59
3.6	Public Sector Applications: From Pilot to Practice.....	61
3.6.1	Synthesizing the Evidence: Patterns and Paradoxes in Public Sector Adoption.....	63
3.7	Decisive Bottlenecks and Systemic Risks in Public Administration	66
3.7.1	Data Protection, Equity, and the Accountability of Automated Law	68
3.8	Conclusion: A Playbook for Legitimate Blockchain Implementation	70
4	<i>Chapter 3: The Algorithmic Leviathan: Code, Consensus, and the Future of Organization in a Decentralized Age</i>	73
4.1	Introduction and Research Context	73
4.1.1	Research Statement and Questions	74
4.1.2	Methodological Framework	75
4.1.3	Contribution	77
4.1.4	Literature Review.....	77
4.1.5	Chapter Structure and Plan.....	79
4.2	The Technology Layer.....	81
4.2.1	The Principle of Decentralization	81
4.2.2	Transparency: The Double-Edged Sword	83
4.2.3	Immutability: The Unyielding Foundation	85
4.2.4	Smart Contracts: The Promise of Autonomous Execution	87
4.2.5	A Systemic Constraint: The Blockchain Trilemma.....	88
4.3	The Governance Layer	90
4.3.1	The Duality of DAO Governance: On-Chain and Off-Chain	92
4.3.2	Consensus and Voting Mechanisms	96
4.3.3	Governance Pathologies and Legitimacy Crisis	98
4.3.4	Polycentric Governance and Digital Commons.....	103
4.3.5	A New Institutional Competitor.....	104
4.4	The Economic Logic of Decentralized Organizations.....	105
4.4.1	Reconfiguring Transaction Costs, Agency Costs, and Property Rights	105
4.4.2	Tokenomics and the Architecture of Incentives	107
4.4.3	Economic Trade-Offs and Systemic Challenges.....	109
4.5	The Practical Manifestations of Decentralized Organizations	111
4.5.1	DAO Typologies	111
4.5.2	DAO Platforms as Enabling Infrastructure	113

4.5.3	Applications in Decentralized Finance	114
4.5.4	Philanthropy DAOs.....	118
4.5.5	Societal Impact DAOs.....	119
4.5.6	Community, Labor, and Network Coordination.....	120
4.5.7	Governance Innovation and Civic Applications	120
4.5.8	Manifestations of Crisis and Confrontation	121
4.6	Conclusion: DAOs as new forms of governance.....	122
5	<i>Chapter 4: Blockchain Technology and Law from the Perspective of Decentralized Autonomous Organizations and the Corporate Law.....</i>	124
5.1	Introduction and Research Context	124
5.1.1	Research Statement and Questions	124
5.1.2	Methodological Framework.....	125
5.1.3	Contribution	126
5.1.4	Literature Review.....	127
5.2	Setting the Stage: Current State-of-Art of DAOs.....	129
5.3	DAOs and Traditional Corporations.....	130
5.4	Legal Personality: The Foundational Challenge for DAOs.....	131
5.4.1	DAOs and the Absence of Personhood	132
5.4.2	The Default Status: General Partnership and Unlimited Liability.....	133
5.4.3	Landmark Legal Precedents and the Reality of Liability.....	134
5.4.4	The "Interface Problem": Practical Impediments.....	135
5.5	Limited Liability: The Protective Veil of Modern Enterprise.....	136
5.5.1	The Corporate Paradigm: The Economic Rationale for Shielding Owners	137
5.5.2	The Inherent Trade-Off: Moral Hazard and Creditor Protection	138
5.5.3	The Native DAO: A Return to an Era of Unlimited Liability	139
5.5.4	The Failure of "Code is Law" as a Liability Shield	139
5.5.5	Broader Implications and the Path Forward.....	141
5.6	Tokens as Transferable Shares	142
5.6.1	The Nature of the Ownership Asset	142
5.6.2	Mechanisms of Transfer and Record-Keeping.....	143
5.6.3	Acquisition and Distribution of Ownership Interests.....	144
5.6.4	Liquidity, Exit, and Market Dynamics.....	145
5.6.5	Rights Conferred by Ownership Interests.....	146
5.6.6	Transferable Ownership	147
5.6.7	Theoretical and Economic Perspectives.....	149
5.6.8	Brief Regulatory Note	149
5.6.9	Conclusion on Transferable Interests.....	150
5.7	Delegated Management from Human Agents to Algorithmic Execution.....	151
5.7.1	The Corporate Paradigm: The Efficiency and Dilemma of the Agency Relationship	152
5.7.2	Corporate Law as a Solution to Agency Costs.....	153
5.7.3	An Ideological Break: Eliminating the Agent.....	154
5.7.4	The New Governance Dilemmas of Direct Democracy	154
5.7.5	The Pragmatic Convergence: The Re-Emergence of Delegation	155
5.7.6	The Legal and Accountability Vacuum	156
5.7.7	Conclusion on the Management.....	156
5.8	Investor Ownership: From Residual Claimants to Participant Governors.....	157
5.8.1	The Corporate Paradigm: The Primacy of the Shareholder as Residual Claimant	158
5.8.2	The Blurring of Roles: The Token Holder as a Hybrid Actor	159
5.8.3	The Nature of Token Ownership: Direct Control and Ambiguous Claims	160

5.8.4	The Legal and Practical Ambiguities of DAO Ownership.....	160
5.9	Conclusion of the Comparative Analysis	161
5.10	Regulatory Landscape for DAOs in the European Union and the United States	162
5.10.1	Federal-Level Approaches in the US.....	162
5.10.2	State-Level Innovations from the US: Laboratories of DAO Law	164
5.10.3	The European Union: A Cautious Integration Approach.....	166
5.10.4	Comparative Reflections: Convergence and Divergence.....	168
5.10.4.1	<i>Toward a Harmonized Regulatory Blueprint</i>	169
5.10.5	Conclusion.....	169
6	Conclusion and Recommendations	171
6.1	Synthesis of Key Findings.....	171
6.2	Recommendations	173
6.3	Contributions, Limitations, and Future Research	174
	<i>Bibliography</i>.....	176

1 Introduction

Few technologies in modern history have arrived with the same profound ideological charge as blockchain. Introduced not merely as an incremental upgrade but as a political proposal to re-architect trust, transaction, and governance, its roots lie in a techno-libertarian cypherpunk movement aiming to replace fallible, human-mediated intermediaries, chiefly states and corporations, with the cryptographic certainty of automated code. This thesis confronts that revolutionary vision with the sober reality of its application. It provides a critical investigation into the profound paradoxes emerging when this radically anti-institutional technology, conceived to operate without central authority, collides with the established structures of both *public governance* and *private governance*.

Emerging from critiques of digital centralization and the perceived failures of institutional trust, particularly highlighted by the 2008 financial crisis, blockchain promised a future of decentralized, self-organizing networks capable of superseding traditional institutions. The core proposition was bold: fundamental functions, from currency issuance to contract enforcement, could be automated via immutable code in a new legal order termed *Lex Cryptographia*, displacing the authority of traditional law and hierarchical management.

This thesis interrogates this transformative vision by examining its encounter with reality, focusing on two primary domains: the constitutional state and the corporate form. The central research question investigates: *How can a technology designed for decentralization and algorithmic immutability be integrated into, or reconciled with, governance systems predicated on centralized authority, legal discretion, and human accountability?* This work explores the deep-seated friction arising when the logic of distributed networks meets the ordered, rights-based framework of public law *and* the established principles of corporate law. It interrogates how blockchain's celebrated virtues, permissionless access, immutability, transparency, become significant liabilities within these regulated and institutionally grounded spheres.

The central argument advanced is that blockchain's integration is predominantly characterized by *cautious institutional adaptation and pragmatic co-option*, rather than revolution. The entrenched normative frameworks of public and corporate law act as powerful constraining forces, compelling the technology to evolve away from its radical origins. In the public sector, this manifests as a domestication into a tool reinforcing state authority, often within New Public Governance (NPG) models. In the private sector, the attempt to instantiate pure decentralized governance via DAOs encounters fundamental legal misfits concerning personhood, liability, and agency, hindering their maturation and forcing hybrid solutions. The observed outcome is less a displacement of traditional structures and more a complex, often paradoxical, negotiation between technological potential and enduring legal and organizational realities.

This study offers a rigorous, multi-disciplinary analysis grounded in legal doctrine, organizational theory, and socio-technical studies, moving beyond speculative hype to examine real-world governance challenges. For policymakers, legislators, and administrators, it provides a clear-eyed assessment of blockchain's true potential and inherent limitations, offering a conceptual framework for responsible implementation that prioritizes legal and constitutional values. For legal, organizational, and political scholars, it contributes to a deeper understanding of institutional

evolution in the face of disruptive technology, detailing how established legal and governance regimes adapt to, shape, and ultimately tame decentralized architectures.

This introductory chapter first outlines the overarching methodology guiding this research (Section 1.1). Subsequently, Section 1.2 presents the structure of the thesis, summarizing the specific focus and contribution of each analytical chapter.

1.1 Notes on Methodology

This thesis employs a *qualitative, interpretive research paradigm* grounded in a *constructivist epistemology*. Its primary aim is to investigate the complex, socially constructed interplay between blockchain technology, law (public and corporate), and governance (state and organizational). The central research questions, concerning the integration of a decentralized technology into centralized legal and institutional structures, are fundamentally about *how* and *why*. They address normative conflicts, meaning-making processes, and institutional adaptations, rather than quantifiable impacts. Therefore, an interpretive approach is essential to understand blockchain not as a predetermined force but as a socio-technical artifact imbued with specific values and reshaped by the environments it encounters.

The research is designed as a *comprehensive, multi-disciplinary, literature-based study* utilizing a method of *thematic synthesis*. This approach is well-suited for a nascent and rapidly evolving field where critical knowledge and empirical data are fragmented across diverse textual sources, including academic scholarship (law, economics, computer science, sociology), legal statutes, court rulings, governmental reports, technical white papers, and foundational philosophical texts. The objective is not merely to review existing literature but to *build theory* by systematically identifying, analyzing, and integrating findings from these disparate sources. This synthesis aims to construct coherent theoretical arguments, such as the "governance paradox" in public law and the "legal misfit" of DAOs in corporate law, that explain observed patterns of adoption, conflict, and adaptation.

The analytical process followed a rigorous three-stage thematic synthesis:

1. **Free Line-by-Line Coding:** Thorough reading and deconstruction of selected texts to identify key concepts, arguments, legal precedents, empirical findings, and design principles related to blockchain, governance, and law.
2. **Organization into Descriptive Themes:** Systematic comparison and grouping of initial codes into hierarchical structures representing recurring, empirically grounded patterns and issues (e.g., preference for permissioned systems, GDPR conflicts, DAO liability defaults, token concentration, re-emergence of delegation).
3. **Generation of Analytical Themes:** Interpretation and synthesis of descriptive themes to generate higher-order analytical themes forming the core arguments of the thesis, constructing overarching narratives about institutional co-option, legal incompatibility, and the negotiation between code and law.

Specific chapters employ tailored analytical lenses within this overarching framework: Chapter 1 uses *narrative and genealogical analysis* to reconstruct blockchain's ideological history. Chapter 2 employs *deep doctrinal and jurisprudential analysis* to juxtapose blockchain properties with public law principles. Chapter 3 adopts a *multi-perspectival framework* (technology, governance, economics, manifestation) grounded in *organizational theory and institutional economics* to analyze DAOs. Chapter 4 uses *comparative legal analysis*, contrasting DAO attributes with foundational *corporate law principles*.

The *primary data sources* are textual and encompass:

- **Doctrinal Legal and Jurisprudential Scholarship:** Foundational and contemporary works on public law, administrative law, constitutional theory, *corporate law*, partnership law, and the emerging field of "blockchain/crypto-law."
- **Organizational and Governance Theory:** Literature on public administration (NPG), theory of the firm (Coase, Williamson), agency theory (Jensen & Meckling), commons governance (Ostrom), and network governance (Powell).
- **Historical, Technical, and Philosophical Literature:** Cypherpunk manifestos, technical white papers (Bitcoin, Ethereum), foundational texts in political philosophy (Hobbes, Rousseau), and critical technology studies.
- **Grey Literature and Empirical Evidence:** Reports from governmental and regulatory bodies (SEC, CFTC, EU Commission, OECD), documentation from pilot projects and specific DAOs, landmark court filings (*Ooki DAO*, *bZx DAO*), policy analyses, and empirical studies on DAO governance metrics (token distribution, voter turnout).

By integrating these diverse sources through thematic synthesis, the thesis aims to provide a robust, theoretically grounded, and empirically informed analysis of blockchain's complex relationship with law and governance.

1.2 Structure of the Thesis / Outlook

This thesis unfolds across four main analytical chapters, each designed to systematically investigate the interaction between blockchain technology and established governance frameworks, progressing logically from foundational ideology to specific legal and organizational challenges.

Chapter 1: The Ideological History of the Blockchain Technology: From Cyberspace to Bitcoin establishes the essential historical and philosophical context. Employing a narrative and genealogical methodology, it argues that blockchain is the material embodiment of a "techno-decentralist ideology" rooted in critiques of centralized state and corporate power. It traces this ideology from early cyber-utopianism and the "Californian Ideology," through the enclosure of the digital commons and the rise of "Rule by Code," to the cypherpunk counter-revolution seeking cryptographic tools for autonomy, culminating in the Nakamoto synthesis (Bitcoin) as a politically charged response to the 2008 financial crisis. This chapter provides the indispensable ideological baseline against which blockchain's subsequent institutional encounters are measured, asking how

critiques of centralization motivated its design and how it operationalizes decentralization as a governance principle.

Chapter 2: Blockchain in Public Governance performs the core theoretical construction regarding the clash between blockchain and *public law*. Using doctrinal and jurisprudential analysis informed by thematic synthesis, it formally develops the "governance paradox." It systematically juxtaposes foundational principles of the constitutional state (rule of law, legality, due process, proportionality, accountability, discretion) against blockchain's inherent properties (immutability, decentralization, transparency, automation). The chapter details fundamental conflicts, particularly the tension between algorithmic rigidity and legal contestability/discretion, and between network decentralization and hierarchical legal responsibility. It situates blockchain within the evolution of public administration paradigms, exploring its alignment with, and challenges to, New Public Governance (NPG), asking how its design logic impacts legality, trust, and automation risks. It concludes by arguing these paradoxes drive adaptation toward controlled, state-overseen implementations.

Chapter 3: The Algorithmic Leviathan: Code, Consensus, and the Future of Organization in a Decentralized Age shifts the focus to *private governance*, examining *Decentralized Autonomous Organizations (DAOs)* as organizational experiments. Adopting a multi-perspectival framework (technology, governance, economics, manifestation) and drawing on organizational theory and institutional economics, this chapter investigates DAOs as attempts to create self-regulating collectives governed by code. It analyzes how core blockchain features enable DAO coordination while also creating paradoxes (e.g., transparency vs. privacy, immutability vs. adaptability, Blockchain Trilemma). It explores the hybridity of on-chain (algorithmic) and off-chain (social) governance, detailing voting mechanisms and identifying persistent pathologies like low turnout and power concentration ("whales"). It connects DAOs to economic theories (transaction costs, agency costs) via "tokenomics" and examines practical manifestations across DeFi, philanthropy, and labor, asking how DAOs operationalize governance, diverge from traditional forms, and reconfigure power.

Chapter 4: Blockchain Technology and Law from the Perspective of Decentralized Autonomous Organizations and Corporate Law confronts the critical legal consequences of the DAO experiment, focusing on the tension with *corporate law*. Using comparative legal analysis, it contrasts the five core attributes of the traditional corporation (legal personality, limited liability, transferable shares, delegated management, investor ownership) with the unique architecture of DAOs. It demonstrates the profound legal misfit, particularly the lack of legal personality and limited liability, leading to the default classification as general partnerships and exposing members to unlimited liability (evidenced by landmark cases). It analyzes the "interface problem," the failure of "code is law" as a liability shield, the re-emergence of delegation without fiduciary duties, and the ambiguous nature of token ownership rights compared to shareholder rights. The chapter evaluates emerging regulatory responses (e.g., US state DAO LLCs, EU's MiCA gaps) and the use of "legal wrappers," asking how effective these solutions are and what a path toward legal certainty might entail.

Finally, the **Conclusion** synthesizes the findings from all chapters, providing a comprehensive answer to the overarching research question about reconciling decentralized technology with

established legal and governance structures in both public and private domains. It summarizes the key arguments regarding the governance paradox, institutional adaptation, the legal misfit of DAOs, and reiterates the thesis's main theoretical and policy implications, offering a forward-looking perspective on the co-evolution of blockchain, law, and organization.

2 Chapter 1: The Ideological History of the Blockchain Technology: From Cyberspace to Bitcoin

2.1 Introduction and Research Context

This chapter examines the ideological history of blockchain technology, situating its emergence within broader political and technological struggles over authority and trust in digital societies. Blockchain is introduced not merely as a computational innovation, but as a socio-technical response to an increasingly centralized digital ecosystem dominated by institutional and corporate power (Nakamoto, 2008; Zuboff, 2023). By reconstructing this genealogy, the chapter demonstrates that blockchain's development is rooted in a deliberate attempt to reconfigure the relationship between individuals, digital intermediaries, and the state. The technology embodies an aspiration to distribute decision-making authority across a network of peers, thereby transforming the very basis upon which trust and coordination are organized (De Filippi et al., 2024; Werbach, 2018).

The narrative begins with the early internet's cyber-utopian ethos, which envisioned cyberspace as a self-governing domain capable of transcending the territorial reach of sovereign states (Barlow, 1996). This vision, however, steadily collapsed under market pressure, network effects, and the rise of platform monopolies that enclosed the once-permissionless digital commons (Barbrook & Cameron, 1996; Parkin, 2020). In response, a technically sophisticated and politically motivated counter-movement emerged in the form of the cypherpunks, who believed that cryptography was the most effective instrument for resisting surveillance and consolidating digital freedom (Hughes, 1993; May, 1992). Their goal was not merely to critique centralization but to build tools that would render external control technically impossible.

Within this lineage, Bitcoin and the underlying blockchain architecture appear as the culmination of a decades-long search for a form of digital coordination that could circumvent gatekeeping institutions and establish an alternative foundation for trust, one based on cryptographic verification rather than legal authority or discretionary human judgment (Nakamoto, 2008; Antonopoulos, 2014). Crucially, this ambition aligns blockchain with long-standing philosophical and economic debates about the nature of sovereignty, and the risks of concentrated power, and the governance of commons (Hobbes & Missner, 2016; Ostrom, 1990). Thus, the chapter argues that blockchain, despite its novelty, extends a much older intellectual trajectory: the quest for decentralization as both a normative principle and a practical mode of organization.

By establishing this historical and ideological context, the chapter lays the conceptual groundwork for the analyses that follow in later chapters. The public-sector applications studied in Chapter 2 and the decentralized private governance experiments in Chapter 3 can only be critically understood by grappling with blockchain's foundational mission: to build governance into the network itself and demonstrate that collective order can arise without institutional sovereignty.

2.1.1 Research Statement and Questions

The central objective of this chapter is to investigate how blockchain technology emerged as a political response to digital centralization, exploring the intellectual currents that shaped its design. Rather than treating blockchain as merely an efficiency-enhancing data structure, the chapter emphasizes the normative commitments encoded into its architecture. Blockchain embeds a form of governance that is executed through protocol rules, cryptographic guarantees, and economic incentives, rather than through state law or corporate authority (De Filippi et al., 2024; Reijers et al., 2021). The core analytical argument is that blockchain represents the materialization of techno-decentralism: a belief that legitimate order can be established through distributed systems in which the need for trust in human actors is minimized.

This focus raises a broader theoretical concern: whether technological infrastructures can fulfill the functions traditionally held by institutions. The shift from law to code, from ex post enforcement through courts to ex ante enforcement through deterministic execution, challenges conventional assumptions about accountability, discretion, and legitimacy (Finck, 2018). Blockchain therefore invites fundamental questions about the kinds of governance arrangements that can meaningfully sustain social cooperation.

To address this, the chapter conducts a historical and conceptual inquiry structured around the following research questions:

1. How did critiques of centralized power and digital enclosure motivate the design goals of blockchain technology?
2. What role did cryptography and distributed networks play as instruments of political resistance within the cypherpunk movement?
3. How did blockchain operationalize decentralization as both a governance principle and a system for institutional coordination?
4. In what ways does blockchain's trust architecture challenge traditional forms of legal and economic governance?
5. How do the philosophical and economic assumptions underlying blockchain shape its contemporary applications?

By answering these questions, the chapter provides a coherent theoretical foundation for examining how blockchain's institutional aspirations evolve in the subsequent analyses of state and private governance.

2.1.2 Methodological Framework

The methodology employed in this chapter is qualitative, interpretive, and historically oriented. Its objective is to uncover how blockchain's technical architecture embodies specific ideological and political commitments, and how these commitments evolved over time through interactions between distributed computing, economic theory, and governance philosophy. This interpretive orientation is necessary because the chapter's inquiry is not concerned with quantifying

blockchain's performance, but with understanding the normative logics that motivated its creation and continue to influence its development (Reijers et al., 2016).

The research proceeds through a narrative and genealogical analysis. It reconstructs blockchain's lineage by tracing key intellectual influences, including cyberlibertarian utopianism, the rise of private digital empires, and cryptographic activism, and analyzing how each movement contributed to the system's design assumptions (Barbrook & Cameron, 1996; Hughes, 1993; Parkin, 2020). Primary sources such as cypherpunk manifestos, technical white papers, and government responses to encryption form the basis for understanding the intentions of early innovators (Chaum, 1983; Electronic Frontier Foundation, n.d.; May, 1992; Nakamoto, 2008). Secondary scholarship in political theory, technology regulation, and institutional economics provides conceptual lenses for making sense of these developments (Lessig, 2009; Ostrom, 1990; Werbach, 2018).

Analytically, the chapter treats blockchain as a hybrid socio-technical system in which rules function simultaneously as computational constraints and political commitments (De Filippi & Wright, 2018). This methodological approach reveals how ideas that were once aspirational, such as the removal of intermediaries or the decentralization of decision-making, became concretized in the mechanisms of consensus, cryptoeconomics, and distributed ledgers.

2.1.3 Contributions

This chapter contributes to the thesis and the field by establishing the historical and ideological foundations necessary to understand blockchain as a governance technology. Its first major contribution is to reposition blockchain within a broader political and institutional narrative, demonstrating that decentralization was not an incidental by-product of technical innovation but the primary normative objective driving its design (De Filippi et al., 2024; Parkin, 2020). A second contribution lies in bridging digital-history scholarship with governance theory, showing how the cypherpunk movement and the Californian Ideology embed assumptions about autonomy, authority, and trust directly into technical architectures (Barbrook & Cameron, 1996; R. Manne, 2020). This synthesis reframes blockchain as an institutional response to the enclosure of the digital commons, motivated by a desire to redistribute power away from state and corporate intermediaries (Lessig, 2009; Zuboff, 2023). Finally, the chapter provides the analytical baseline against which the next chapters evaluate blockchain's institutional claims in practice: Chapter 2 tests these aspirations within public administration, while Chapter 3 examines whether decentralized organizations can operationalize these ideological commitments in real-world economic and organizational contexts. Through this contextual foundation, the chapter ensures that subsequent legal and governance analysis remains grounded in the political origins that continue to shape blockchain's development trajectory.

2.1.4 Literature Review

Academic scholarship on blockchain's origins is inherently interdisciplinary, spanning political philosophy, critical technology studies, cryptography, and institutional economics. Across these domains, a shared understanding emerges: blockchain technology is a socio-technical artifact created in response to the progressive centralization of digital power and the erosion of individual autonomy online (De Filippi et al., 2024; Zuboff, 2023). The literature thus converges on the view that blockchain is not merely a technical system but the material embodiment of a political critique and an institutional aspiration.

The first major thread of literature examines *cyber-utopian imaginaries of the early internet*, which framed cyberspace as a sovereign and liberatory environment. Barlow's (1996) iconic "*Declaration of the Independence of Cyberspace*" crystallized a belief that digital networks could establish self-governing spaces insulated from state authority. Barbrook and Cameron (1996) characterize this as the "Californian Ideology," a paradoxical fusion of counterculture libertarian ideals and Silicon Valley entrepreneurialism that promoted both radical freedom and market determinism (Parkin, 2020). These narratives positioned decentralization as the natural state of the digital realm, where technological affordances would render old power structures obsolete.

However, a second critical body of scholarship documents how these utopian ambitions gave way to *platform centralization*, fueled by network effects, economies of scale, and the commodification of user data (Werbach, 2018; Zuboff, 2023). Research shows that the open architecture of the early internet was progressively enclosed within corporate-controlled ecosystems, producing unprecedented concentrations of infrastructural and epistemic power (Srnicek, 2017). Lessig (2009) argues that digital architecture, "code", emerged as a foundational modality of regulation, capable of coercively shaping behavior without democratic oversight. This literature portrays the internet's evolution as a cautionary tale: decentralization is not a default but a fragile ideal continuously threatened by market logics and governance asymmetries.

Motivated by this consolidation of digital control, a robust scholarly discourse examines the *cypherpunk movement* as the ideological and technical precursor to blockchain. The cypherpunks operationalized cryptography as a tool of political agency, enabling resistance to surveillance and censorship (Assange et al., 2016; Magnuson, 2020). Their manifestos emphasized privacy as a self-help responsibility and insisted that code, not law, would secure digital freedom (Hughes, 1993; May, 1992). Historical research highlights iterative technological experiments with decentralized digital cash, including Chaum's *eCash*, Back's *Hashcash*, Dai's *b-money*, and Szabo's *Bit Gold* (Chaum & Brands, 1997; Back, 2002; Dai, 1998; Szabo, 1997). Although these prototypes failed to achieve full decentralization, they provided the conceptual ingredients later synthesized by Bitcoin.

A further scholarly strand interprets blockchain as part of *institutional economics and governance theory*. Works, such as the ones drawing on Ostrom (1990), emphasize how blockchain embeds alternative mechanisms for the governance and enforcement of rules in polycentric and network structures (Ostrom, 1990; Powell, 1990). Blockchain's cryptoeconomic incentives function as institutional substitutes for trust and monitoring, enabling large-scale cooperation among pseudonymous actors (De Filippi & Wright, 2018). This perspective positions blockchain

protocols as “economic constitutions,” where governance is automated through transparent constraints rather than hierarchical command.

Finally, contemporary socio-technical scholarship argues that blockchain inaugurates *a new form of political order*: governance executed through infrastructure itself (Reijers et al., 2021; De Filippi et al., 2024). By collapsing the distinction between institution and network, blockchain aspires to achieve what Lessig (2009) called “perfect enforcement”, leaving no room for discretion, contextual interpretation, or lawful exception (Finck, 2018). This raises normative questions about legitimacy, accountability, and the preservation of fundamental rights when governance becomes embedded in immutable code.

Taken together, the literature portrays blockchain’s invention as a historically contingent response to a governance crisis in digital society. The technology is a counter-proposal to centralized platforms and a continuation of longstanding philosophical debates about authority, freedom, and the possibility of self-organizing communities at scale. Blockchain’s institutional implications, central to the following chapters, cannot be understood apart from this ideological and political lineage.

2.1.5 Chapter Structure and Plan

This chapter is structured to unfold the evolution of blockchain’s ideological foundations in a coherent and escalating conceptual arc. It proceeds from early political imaginaries of decentralized cyberspace to the concrete cryptographic innovations that operationalized those imaginaries in Bitcoin. The progression is designed to demonstrate how ideas transformed into technical architectures and how those architectures, in turn, express institutional commitments that shape governance in the digital realm.

The chapter begins with a historical analysis of *cyber-utopianism and digital sovereignty*, showing how early internet pioneers envisioned a borderless environment governed by voluntary association rather than state authority (Barlow, 1996). This section establishes decentralization as initially grounded in political and cultural aspirations rather than technical necessity. It also highlights the paradoxes and ideological tensions embedded within the Californian Ideology, which simultaneously celebrated radical autonomy and unregulated capitalism (Barbrook & Cameron, 1996; Parkin, 2020).

The chapter then transitions to a critical account of *the enclosure of the digital commons*, documenting how the liberatory architecture of the early internet shifted into privately controlled infrastructures driven by market imperatives. This section demonstrates that digital power progressively consolidated through platform monopolies, surveillance capitalism, and code-based rule enforcement (Lessig, 2009; Zuboff, 2023). It frames blockchain as a reaction to these governance failures, a technological rejection of systems that concentrate authority without accountability.

Building upon this critique, the chapter next examines *the cypherpunk counter-revolution*. Here, cryptography emerges as a political strategy for preserving individual autonomy against institutional encroachment. The discussion traces the development of digital-cash prototypes, showing how the cypherpunks sought not policy reform but technological transcendence of state and corporate power (Assange et al., 2016; Hughes, 1993). The analysis emphasizes that this movement was grounded in direct technological action, “Cypherpunks write code”, rather than abstract idealism.

The penultimate section focuses on *the Nakamoto synthesis*: the moment in which Bitcoin unified decentralized networking, cryptography, and economic incentives into a self-regulating system capable of maintaining an authoritative ledger without a central intermediary (Antonopoulos, 2014; Nakamoto, 2008; Narayanan et al., 2016). This section demonstrates how blockchain represents the technical institutionalization of decentralization, embedding governance directly into protocol design.

The chapter concludes by synthesizing these developments into a conceptual claim: blockchain represents a new institutional paradigm in which governance is executed through cryptographic infrastructure rather than legal or hierarchical authority. This synthesis situates blockchain as the conceptual baseline for the thesis. It prepares the analytical transition to *Chapter 2*, where blockchain’s ideological promises are tested within public-sector governance systems, *Chapter 3*, where the technology’s anti-statist aspirations encounter the realities of decentralized private organizations, and *Chapter 4* when these realities crash with the law.

2.2 Setting the Stage: The History of Blockchain Before Blockchain

Historically, the promise of decentralization has been a recurring theme, invoked whenever new technologies emerge that appear to challenge concentrated power, whether held by the state or by dominant corporations. This continuous philosophical debate over where power should reside in modern society is a central animating force of technological development (De Filippi et al., 2024). Technologies that offer greater individual control and access have always carried significant appeal for the people and society. The printing press, for instance, is widely recognized for having decentralized the dissemination of knowledge on a previously unimaginable scale, thereby challenging the traditional monopolies on information control held by religious and state authorities (De Filippi et al., 2024). Centuries later, the early internet, built on open and permissionless protocols like TCP/IP, was perceived by many as the ultimate instrument of decentralization, promising a global digital commons free from any central point of control (Parkin, 2020). Blockchain technology, therefore, represents the latest chapter in this ongoing struggle, emerging from the perceived failures of these earlier technologies to deliver on their promise of a lasting redistribution of power away from entrenched elites.

The contemporary blockchain movement, while seemingly novel, is built upon decades of prior experimentation with technologies designed to distribute computational and communication power. The fundamental technical architecture of any blockchain relies on distributed peer-to-peer (P2P) software, in which each computer, or node, maintains a replicated copy of the shared ledger

in a structure that has no inherent hierarchy among its peers. This model is not new; early conceptualizations of decentralized networks predate the modern internet, such as those developed by Paul Baran for the RAND Corporation as a resilient communications system in the event of nuclear war (Baran, 1962). Moreover, cybernetics, the study of control and communication in complex systems, has long examined how the interactions between group-level and individual-level processes can give rise to purpose-driven self-organization (Ashby, 1956; Wiener, 2019). From this perspective, blockchain technology represent a modern digital expression of a long-standing political desire for groups to self-organize, mediated by new technological tools (Zargham & Nabben, 2022). Furthermore, the entire ecosystem relies on an open-source software model, which rhetorically promotes egalitarian principles and distributed power among its creators, and on the use of strong cryptography, which was advocated as a political tool for freedom and privacy by the cypherpunks, a group whose intellectual lineage is central to this history (Hughes, 1993).

2.2.1 Early Visions of a Decentralized Cyberspace

The initial perception of the digital realm, or cyberspace, was steeped in a profound techn-utopianism. This worldview was characterized by a language of revolutionary change, linking the mastery of new technologies directly to the achievement of a common good (Barbrook & Cameron, 1996). Early internet culture framed cyberspace as a utopian and self-governing domain, often imagined as an anti-materialist representation of "digital frontier" that has the potential to free society from the conventional limitations of geography and physical power (Dyson, 1996; Parkin, 2020). Especially during the latter half of the 20th century, the San Francisco Bay Area was an important hub where the 1960s liberal, counterculture air intersected with the burgeoning fields of computer technology and entrepreneurship (Barbrook & Cameron, 1996).

This ideological blending took place when the developments in the computer science combined with communist and liberalist ideals, allowing the internet to emerge as a representation of a "youthful revolution reborn" (Turner, 2024). By the late 1980s, a new generation of cyberlibertarians began to regard the internet as a new territory that promised liberation from traditional authoritative bonds (Featherstone & Burrows, 1995). Influential figures like Stewart Brand actively worked to fuse countercultural ideals, such as communal living and consciousness exploration, with the potential of advanced electronic networks (De Filippi et al., 2024). This effort was instrumental in reimagining computers, once widely seen as tools of dehumanizing mechanization and bureaucratic control, as powerful instruments for fostering communal connection and expanding individual freedom, thereby setting the stage for the creation of new alternative communities online.

This view of cyberspace as a sovereign, ungovernable realm was powerfully crystallized in 1996 by John Perry Barlow, a founder of the Electronic Frontier Foundation (EFF), in his essay, "*A Declaration of the Independence of Cyberspace*" (Barlow, 1996). In a direct challenge to state authority, Barlow proclaimed: "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of*

the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." This manifesto, utilizing an allegorical tone reminiscent of Thomas Jefferson and the colonial expansion into the American West, declared that the global social space being built online was "*naturally independent of the tyrannies*" that governments sought to impose upon it (Parkin, 2020; Finck, 2018). Barlow's position was that individual sovereignty in this new domain was neither derived from nor subordinate to the sovereignty of any state (De Filippi et al., 2024). These ideas became emblematic of cyberlibertarianism, an ideology that linked the enthusiastic adoption of electronic life with the libertarian concepts regarding freedom, economics, and politics (Barbrook & Cameron, 1996).

2.2.2 The Californian Ideology

The intellectual product of this unique cross-fertilization of counterculture and entrepreneurial drive was critically termed the "Californian Ideology" by scholars Richard Barbrook and Andy Cameron (Barbrook & Cameron, 1996). Their critique aptly encapsulated the libertarian-entrepreneurial principles that were starting to permeate the fledgling technology sector (Parkin, 2020). The philosophy, which was characterized as a "contradictory blend of conservative economics and hippie radicalism", was able to bring the aggressive, market-driven entrepreneurial zeal and the free-spirited, anti-authoritarian principles together (Barbrook & Cameron, 1996). This peculiar meeting led to the rise of the cybernetic libertarianism, which mixes economic liberalism with hippie anarchism and bolstering it with a profound sense of technological determinism (Parkin, 2020).

The foundation of this philosophy was an unwavering trust in the potential of new information technologies (Barbrook & Cameron, 1996; Parkin, 2020). It fostered the belief that technology, if efficiently deployed, could offer definitive "solutions" to problems that were traditionally confined to the messy and complex realm of human politics (Hillis et al., 2012). This framework created a direct and untroubled alignment between the concept of 'free' markets and that of personal 'freedom,' which had the consequential effect of legitimizing new, centralized concentrations of power, provided they were determined by market forces and "voted for by dollars" (Parkin, 2020). Drawing heavily on the writings of figures like Ayn Rand, this worldview promoted radical individualism and a deep distrust of centralized state control as the essential keys to a truly free society (Parkin, 2020). This utopian vision, however, would soon be questioned, as the idea that code alone could guarantee freedom met the "cold hard limits of reality" (Werbach, 2018). Critics correctly anticipated that the internet, despite its initial design for fostering freedom, would eventually become centralized and subjected to the control of a handful of powerful corporate entities, proving that code, while a powerful force, does not in itself eliminate hierarchy or the relentless pursuit of power (Poncibò, 2020).

2.2.3 The Enclosure of the Digital Commons

The initial utopian vision of cyberspace as a self-governing and decentralized domain rapidly confronted the formidable commercial realities of the digital economy. This collision resulted in a profound and definitive shift away from an open, shared infrastructure toward a landscape of closed, corporate-controlled spaces. While the early internet was characterized by decentralized protocols that facilitated permissionless innovation, the combined forces of technological maturation and market logic steered development inexorably toward centralized organizations. This process is best understood as the enclosure of the digital commons. The foundational ideals of the early internet had promoted the concept of a "digital commons," which was envisioned as an open, diverse, and free network, akin to a thriving and ungated forest (Cappiello & Carullo, 2021). The underlying infrastructure, such as the TCP/IP protocol, was designed to be a neutral and open foundational layer upon which anyone could build.

In stark contrast, the phenomenon of "digital enclosure" describes the subsequent erosion of this openness and the establishment of proprietary points of control that effectively privatized the digital frontier. This enclosure occurs when decentralized systems are gradually molded and ultimately dominated by centralized governments, software platforms, and data centers (Clayton et al., 2006). Despite the internet having been built on distributed protocols, its practical utility for everyday users became dependent on a few curated service platforms that simplified access and navigation. This process ensured that online interactions became increasingly financialized, with a small number of powerful gatekeepers coming to control vast and growing repositories of citizen data (Werbach, 2018). This transformation echoes historical processes, most notably the land enclosures of previous centuries, whereby shared resources were systematically converted into private holdings for commercial exploitation. In a similar vein, the ideological shift resulting from the fusion of counterculture and capitalism led directly to the "colonisation of the Net by corporate behemoths" (Barbrook & Cameron, 2015). This new concentration of power is captured in critical terms like "cloud empires" and the related concept of "techno-feudalism," which describes a shift in the digital realm away from traditional capitalistic competition and toward rent-seeking and the expropriation of data from a dependent user base (De Filippi et al., 2024).

2.2.4 Network Effects and Winner-Takes-All Dynamics

The systemic shift toward enclosure was not accidental but was dramatically accelerated by fundamental economic dynamics specific to networked systems, most importantly the principle of network effects. A network effect is a phenomenon whereby a platform or service increases in value in direct proportion to the number of users it enrolls (Belleflamme & Peitz, 2018). Each new user on a social media platform, for instance, makes the platform more valuable for all existing users by expanding the pool of potential connections. This dynamic leads directly to winner-takes-all scenarios, where the largest network becomes exponentially more attractive than its smaller competitors, creating a powerful gravitational pull. An established network offers immense value to new entrants while simultaneously imposing a high cost on existing members who might consider leaving, effectively locking in users through social and economic inertia (Varga et al., 2023).

This powerful first-mover advantage was seized by early entrants, the Big Tech companies, who benefited enormously as the internet scaled. The natural consumer preference for coherent ecosystems and easy-to-use interfaces further reinforced this trend, pushing even technologies that were architecturally decentralized in a functionally centralized direction (De Filippi et al., 2024). As a result, a few giant corporations, often countable on a single hand, came to dominate the core functions of the digital economy, controlling critical sectors like social media with Facebook, online search with Google, and e-commerce with Amazon. This represented an unrivaled consolidation of market power, creating new monopolies from the decentralized beginnings of the internet and demonstrating that the struggle between centralized and decentralized forces is often cyclical.

2.2.5 Platforms, Privatization, and Governance by Code

The corporate platforms that emerged from these dynamics enforced their control by privatizing user data and establishing *walled gardens*, closed ecosystems designed to keep users within a proprietary environment (Werbach, 2018). The business model that powered this enclosure is now widely understood through the lens of "*surveillance capitalism*," a term popularized by Shoshana Zuboff. Surveillance capitalism defines a digital economic logic reliant on the commodification of personal information for profit and the subsequent regulation of user behavior asset (Zuboff, 2023). In this model, platform owners extract immense amounts of data, which is treated as a valuable raw material to be refined and monetized (Srnicek, 2017). The foundational business structure of these "*cloud empires*" depends on the suppression of privacy to generate revenue streams sold to advertisers and market researchers, transforming personal information into a commercial asset (Zuboff, 2023).

These platforms impose hierarchical business models onto the distributed mesh network of the internet, using proprietary interfaces and software to enclose vast sections of the network (Werbach, 2018). They then leverage their control over this infrastructure to dictate the rules of engagement for all participants. Online operators utilize code to precisely stipulate what users can and cannot do on their platforms, a mechanism often described as the "*rule by code*." This governance regime allows operators to exercise full discretionary power over codified rules, primarily to serve their own economic or political interests without external accountability or the checks and balances afforded by public law (De Filippi et al., 2024). In this environment, private sovereignty, exercised through binding and often opaque Terms of Service agreements, effectively replaces public sovereignty as expressed through the rule of law (Finck, 2018).

2.2.6 The Democratic and Societal Implications

The centralization of power in the hands of a few corporate platforms carries significant and troubling democratic implications, particularly concerning information control, censorship, and rising economic inequality. By shaping the information diets of billions of users, these platforms

control how people see the world (Werbach, 2018). They act as "algorithmic gatekeepers," using proprietary and often undisclosed algorithms to filter, highlight, or suppress information, thereby exercising an immense and unaccountable editorial role in global information flows (De Filippi & Wright, 2018). This control is not limited to commercial concerns; these centralized companies also serve as convenient chokepoints for governments seeking to enforce legislation, such as mandating censorship on dominant communication platforms.

The concentration of data and power inherent in this model also enables intrusive forms of surveillance and opens the door for political manipulation and the spread of fake news, as evidenced by controversies such as the Cambridge Analytica scandal (Werbach, 2018). Furthermore, the rise of corporate platforms has dramatically exacerbated economic inequality. These entities capture an enormous share of advertising and transaction revenues, leading to a profound dislocation where the value generated online flows increasingly to the masters of search and platform infrastructure, and not to the content contributors who provide the critical source of that value (Pasquale, 2015). This dynamic contributes to a widening gap between the economic "haves and the have nots," while the market-driven logic of the Californian Ideology often serves to legitimize these powerful centralized positions as a valid expression of consumer choice (De Filippi & Wright, 2018; Parkin, 2020).

The enclosure of the digital commons and the resulting centralization of power in private platforms are rooted in the realization that control within a digital environment is exercised not just through legal rules or market forces, but most fundamentally through the environment's architecture, the code itself. This understanding provides the theoretical key to unlocking how platform dominance was achieved and why it has proven so resilient to challenge. The norms, constraints, and possibilities of cyberspace are written directly into its infrastructure, making the design of that infrastructure an inherently political act.

2.2.7 Code is Law

The central theoretical concept for understanding digital governance is Lawrence Lessig's seminal aphorism, "Code is law" (Lessig, 2009). Lessig argued that software code is a potent and often invisible regulatory force, acting as one of four key mechanisms, alongside traditional law, social norms, and markets, that constrain human action. In cyberspace, code dictates behavior by setting the parameters of what is possible. It can enable certain actions while making others impossible, thereby shaping the human experience in a manner that is functionally equivalent to regulation (A. Zwitter & Hazenberg, 2020b). From this perspective, the architectural choices made by programmers and platform owners are not neutral technical decisions; they are a form of private legislation that determines the rules of engagement for all users.

This architectural control is evident across the digital landscape. Online service providers utilize proprietary code as new and powerful means of regulation, effectively acting as *de facto* regulators that define the rights of users and the acceptable modes of social interaction (A. Zwitter & Hazenberg, 2020b). Ride-sharing platforms like Uber, for instance, rely on code not only to enforce internal conduct rules but also to manipulate drivers' behavior through automated

mechanisms, such as delisting them for failing to adhere to platform-defined metrics (Finck, 2018). Similarly, search engines and social media feeds deploy sophisticated algorithms to filter, spread, and frame information, influencing individual decision-making and shaping user behavior in ways that align with their commercial objectives (Nabben, 2021). A particularly clear example is the use of Digital Rights Management (DRM) systems, which embed the provisions of a copyright license directly into the code of a digital work (De Filippi & Wright, 2018). These systems represent a form of private ordering where computer code can interpret and enforce legality differently from the state, often imposing greater restrictions than national copyright laws would permit by precluding uses that might otherwise be protected under the legal doctrine of fair use (Finck, 2018; De Filippi et al., 2024).

A critical distinction between regulation-by-code and regulation-by-law lies in their enforcement mechanisms and timing. Traditional legal systems operate *ex post*, meaning they punish a violation after it has occurred through the intervention of a third-party authority like a court (De Filippi & Wright, 2018). Law is written in natural language, which is inherently flexible, ambiguous, and subject to contextual interpretation (Finck, 2018). It sets behavioral specifications that individuals have the freedom to disregard, provided they are willing to accept the consequences. In contrast, code regulates *ex ante*; its enforcement is automatic, deterministic, and immediate. The underlying network executes the code exactly as written, often making compliance the only available option for the user (Finck, 2018). Code is written in a strict, formalized language and lacks the capacity to account for nuance, contingency, or legal gray areas, operating with a perfect enforcement that preempts any conduct falling outside its predefined parameters (De Filippi & Wright, 2018).

2.2.8 Rule by Code

While code functions as a powerful source of governance, the decisions regarding its design and implementation on centralized platforms are typically made by private actors who lack democratic oversight and transparency. This concentration of power leads to a regime that has been termed the "Rule by Code," a model in which online operators wield full discretionary power over the rules they codify into their platforms (De Filippi et al., 2024). These private actors, primarily serving their own economic or political interests, exercise an unaccountable editorial role in shaping information flows and social interactions (De Filippi et al., 2024). This system operates without the external accountability or checks and balances that are fundamental to the "rule of law." The technical parameters of the software are determined by a small number of developers, who are often seen as operating as the effective legislative power of these networks (De Filippi & Wright, 2018). The values and biases of these creators become imbued into the algorithmic rules, turning the platforms into "black boxes" whose internal workings are opaque and difficult to scrutinize (Finck, 2018). This concentration of control in a small technocratic class risks creating an algocracy: a social structure governed by rigid, formalized, code-based rules to the detriment of human discretionary choice and democratic ideals (Wood, 2014). This system of architectural control is inextricably linked to the economic model of surveillance capitalism, which thrives on a profound asymmetry of knowledge (Zuboff, 2023).

In this regard, the contemporary digital world has been described as resembling a "one-way mirror" (Pasquale, 2015). While citizens are increasingly tracked by corporations and governments, they remain largely unaware of how far this aggregated information travels, how it is ultimately used, or the consequences of its application. Corporate actors possess unprecedented knowledge of the minutiae of users' daily lives, while users know very little about how this knowledge influences the decisions made about them (Pasquale, 2015). This asymmetry is deliberately reinforced by secrecy and the complexity of proprietary algorithms, which are shielded behind the veil of closed-source software code to confound regulation and maintain a crucial information advantage (Nabben, 2021). The dangers presented by this centralized "Rule by Code", where private entities wield legislative power without public accountability, fueled by an extractive data economy, vividly highlight the necessity for alternatives. It was in direct response to these conditions that a movement emerged with a radical ambition: to use code to free from this unbalanced power dynamics.

2.3 The Cypherpunk Counter-Revolution

The concept of algorithmic decentralization, which forms the bedrock of modern blockchain technology, did not emerge from a corporate research lab or a university computer science department. It has deep ideological roots in a specific, politically motivated movement of programmers, activists, and cryptographers who came to be known as the cypherpunks. This movement, which flourished in the 1990s, served as the direct ideological and technical precursor to Bitcoin and the subsequent explosion of blockchain applications. Acting in direct response to the growing enclosure of the internet and the nascent threat of mass surveillance, the cypherpunks believed that strong cryptography was the essential and necessary tool for achieving individual liberation and autonomy in the dawning digital age (Assange et al., 2016; Magnuson, 2020).

2.3.1 Origins, Ethos, and the Mailing List

The cypherpunks emerged as fiercely independent and anarchist community advocated the use of strong cryptography and privacy-enhancing technologies as tools to promote individual freedom and protect personal privacy in the digital age. Their central aim was to harness technology, specifically cryptography, as a means of liberation of the Internet and communication technologies from the oppression of governments and capitalist companies, as the state and large corporations started to wield unprecedented surveillance power over the individuals. The community became more organized and visible when a mathematician, Eric Hughes, invited programmers with similar motivations to his home in 1992 (R. Manne, 2020). Key figures in this founding group included Timothy May, a former chief scientist at Intel, and John Gilmore, an early employee of Sun Microsystems and a co-founder of the Electronic Frontier Foundation (EFF), an organization devoted to promoting internet freedom (Magnuson, 2020).

These individuals shared a particular and profound interest in cryptography, the study of securing communications from eavesdroppers. At that first meeting, Hughes and May conceived of creating

an electronic mailing list where interested parties could share their thoughts and code related to cryptography, computers, politics, and privacy. Gilmore hosted this crucial communication tool on his personal website, and the list quickly became the vibrant heart of the movement, growing from just over seven hundred subscribers in 1994 to two thousand by 1997 (Magnuson, 2020). This mailing list was the direct predecessor to the one where, over a decade later, the pseudonymous Satoshi Nakamoto would announce Bitcoin to the world. The participants were generally starkly anti-government, sometimes to the point of anarchism, and were animated by a deep-seated paranoia about government snooping and control over digital communications (Magnuson, 2020).

2.3.2 The Foundational Manifestos

The cypherpunks translated their political philosophies into a clear program for action through two key manifestos that defined the movement's ethos. The first, Timothy May's *Crypto Anarchist Manifesto*, was read aloud at the inaugural cypherpunk gathering in 1992. In it, May declared that a "specter is haunting the modern world, the specter of crypto anarchy," and predicted that advances in cryptography would fundamentally alter "the nature of government regulation, the ability to tax and control economic interactions, [and] the ability to keep information secret" (May, 1992). He argued that computer technology was on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner, making the spread of this freedom inevitable. He drew a powerful historical analogy, comparing the future effect of cryptologic methods on society to how the invention of the printing press had irrevocably altered the power structure of medieval guilds and the social power of the church.

A year later, Eric Hughes penned *A Cypherpunk's Manifesto* to unify the group's message and purpose (Hughes, 1993). In this concise and powerful text, he championed the protection of privacy as essential for an open society in the electronic age. Hughes stressed that privacy could not be expected as a gift from benevolent corporations or governments; rather, it had to be actively built and defended by individuals. He wrote, "We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy... We must defend our own privacy if we expect to have any. We the Cypherpunks are dedicated to building anonymous systems." This sentiment culminated in the definitive phrase that encapsulated the movement's profoundly pragmatic and action-oriented ethos: "*Cypherpunks write code*". They were not interested in simply debating policy or lobbying politicians; their method of political resistance was to build the tools that would make surveillance and control impossible. They published their code freely for anyone to use, ensuring their creations could be adopted, adapted, and spread across the globe (Hughes, 1993).

2.3.3 The Crypto Wars and Resistance to State Control

The cypherpunk movement emerged alongside and was a key combatant in the intense political struggles over governmental control of encryption technology, a period often referred to as the “crypto wars” (Electronic Frontier Foundation, 2025). The movement’s ultimate product was the software package PGP, or Pretty Good Privacy (Zimmermann, 1995). Since the government had categorized strong cryptography as a munition, which is legally equal to a weapon, its creator, Phil Zimmermann, was the focus of a three-year criminal investigation that started in 1993 for a potential violation of US export rules (Parkin, 2020). To ingeniously circumvent this control, supporters began printing the entire source code of PGP into books, which could be legally exported abroad and then scanned by recipients to reconstitute the software, highlighting the absurdity of regulating information as a physical weapon.

This battle intensified with the US government's proposal of the Clipper Chip, an encryption device designed by the National Security Agency (NSA). The government attempted to mandate that all manufacturers of communications hardware incorporate this chip, which contained a technological “backdoor” that would allow law enforcement and intelligence agencies to decrypt any and all materials (Electronic Frontier Foundation, 2025). The cypherpunks saw this as a direct assault on digital freedom and privacy. By mobilizing through the EFF and relentlessly advocating for and designing their own independent cryptography systems like PGP, the cypherpunks were instrumental in defeating these early attempts at government control, and the Clipper Chip proposal was ultimately shelved. These chain of actions demonstrated that cryptography is not only a technical tool, but also a political tool against the unbalance between the governments, private companies and the data subjects, which illustrated that private, secure communication should be a right to be defended (Assange et al., 2016).

2.3.4 The Search for Digital Cash

The cypherpunk ethos was, above all, pragmatic. Their goal was not merely to debate political philosophy but to build working alternatives that would render the existing systems of control obsolete. Their ultimate tool of resistance was cryptography, which they viewed as the foundation for societal change and the highest form of non-violent direct action (Assange et al., 2016; Parkin, 2020). While they developed various privacy-enhancing software tools like secure email and anonymous remailers, their most ambitious and challenging project was the creation of a truly anonymous, secure, and decentralized form of digital cash (Magnuson, 2020; Parkin, 2020). For years, they devoted significant effort to developing prototypes that could function as a stateless currency, free from the control of banks and governments. These early attempts, while ultimately unsuccessful, were critical experiments that laid the intellectual and technical groundwork for the eventual invention of Bitcoin.

One of the earliest and most influential pioneers was the cryptographer David Chaum. As early as 1983, Chaum conceptualized a system called eCash, which he later launched through his company DigiCash in 1990. The system was revolutionary for its use of “blind signatures,” a cryptographic technique that allowed a bank to sign a digital token without being able to see its contents, thereby creating a form of anonymous and untraceable digital payment (Chaum, 1983). For all its cryptographic elegance, however, DigiCash had a fatal flaw in the eyes of the cypherpunks: it was

centralized. The system relied entirely on Chaum's company to act as a central clearinghouse to validate every transaction and prevent counterfeiting (Chaum & Brands, 1997). When the company filed for bankruptcy in 1998, the entire currency system crumbled, powerfully reinforcing the cypherpunk conviction that any system with a single point of failure, whether corporate or governmental, was doomed to be co-opted or destroyed.

Another critical piece of the puzzle emerged in 1997 when Adam Back proposed Hashcash. Originally designed as a counter-measure to email spam and denial-of-service attacks, Hashcash introduced an early form of the concept now known as "proof-of-work" (Back, 2002). The idea was to require a sender to perform a small, but not insignificant, amount of computational work, solving a mathematical puzzle, before their email would be accepted. This attached a small real-world cost, in the form of electricity and processing time, to the act of sending a message. While its initial application was for spam filtering, its implication for digital currency was profound. By making the creation of a digital token costly, proof-of-work provided a way to create programmable scarcity and a mechanism to mitigate the *"double-spending problem"* without a central authority. An adaptation of this very system would later become the core of Bitcoin's mining process (Back, 2002).

Building on these ideas, members of the cypherpunk mailing list proposed more comprehensive systems. In 1998, Wei Dai, a famously private computer engineer, conceptualized a digital currency he called "b-money." His proposal outlined a system where transactions would be publicly broadcast to all participants across a peer-to-peer network and recorded in a shared ledger, controlled collectively by the users (Dai, 1998). It was a visionary concept that included many of the architectural elements of modern cryptocurrencies, but it remained a theoretical proposal. It required a Hashcash-like proof-of-work system to create money but lacked a clear, robust mechanism for ensuring all participants agreed on the state of the ledger in the face of network delays and potential attacks.

Around the same time, another foundational thinker in the space, Nick Szabo, conceptualized *"Bit Gold"*. Szabo, who had also invented the concept of the "smart contract" in 1997, envisioned a digital currency that would hold value due to its programmed scarcity, much like a precious metal (Szabo, 1997). His design involved using a proof-of-work function to create unforgeable chains of data, with each link in the chain secured with timestamps and digital signatures. This structure was remarkably similar to the blockchain data structure that would later be formalized in the Bitcoin white paper. However, like b-money, Bit Gold was never fully implemented and suffered from unresolved theoretical issues, particularly in creating a reliable system for network consensus.

The final major precursor was developed in 2004 by Hal Finney, a prominent cypherpunk and one of the first developers of PGP. His system, called Reusable Proof-of-Work (RPOW), ingeniously combined several of the preceding cryptographic developments to create a practical system where digital tokens could be owned and traded between users (Parkin, 2020). Yet, for all its sophistication, RPOW still fell short of the ultimate goal of true decentralization. It relied on a centralized, trusted server to verify the proofs-of-work and ensure that no one could spend the same token more than once (De Filippi et al., 2024). This final failure underscored the central, persistent challenge: how to create a coherent, globally agreed-upon ledger without trusting any single party. All the good, the bad, and the ugly of the cypherpunks' idea bank, blind signatures,

proof-of-work, peer-to-peer ledgers, and chained transactions, went into the *"intellectual soup from which bitcoin would emerge"* (Parkin, 2020). The individual components were all present, but it would take a final, brilliant synthesis to combine them into a working system that finally realized the long-sought dream of digital cash.

2.4 The Nakamoto Synthesis: The Invention of Blockchain

The transition from the ideological pursuit of anonymous digital cash by the cypherpunks to the development of a viable, working system culminated with the introduction of the Bitcoin protocol. This final breakthrough was not the result of a single, novel invention, but rather a brilliant and elegant synthesis of the cryptographic theories, peer-to-peer architectures, and economic incentives that had been developed and debated for years. It was a solution that arrived at a moment of profound political and financial turmoil, giving its technical design an immediate and powerful ideological resonance.

2.4.1 Bitcoin as a Response to Financial Crisis and Distrust

The emergence of Bitcoin after the 2008 global financial crisis was not a coincidence. The motivation behind the development of this technology was explained by Nakamoto as to remove the need for the very institutions that were widely seen as having caused the crash through a combination of recklessness, opacity, and greed (Nakamoto, 2008). The crisis precipitated a profound loss of public trust in centralized authorities, particularly in the global banking system and the governments that were forced to bail them out, revealing the inherent fragility of traditional trust architectures (Werbach, 2018). It was against this backdrop that the pseudonymous creator, or creators, known as Satoshi Nakamoto posted the white paper for Bitcoin on a cryptography mailing list on October 31, 2008.

The underlying political motivation of the project was made explicit from its very first moments of operation. The genesis block, the first block of transactions ever mined on the Bitcoin network, contained an embedded and politically charged message referencing a headline from a UK newspaper: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* (Parkin, 2020). This message served not only as irrefutable proof of the network's launch date but also as a direct and intentional critique of the centrally controlled financial system. It was a commentary on the "too big to fail" mentality and the use of taxpayer money to rescue the very institutions that had failed the public trust (Parkin, 2020). Nakamoto articulated this motivation clearly in later writings, stating that the "root problem with conventional currency is all the trust that's required to make it work" (Nakamoto, 2008). The solution offered was not a plea for reform, but a technical disruption launched from the bottom up by "hackers," using computer code as their instrument.

2.4.2 Weaving the Threads

The Bitcoin software, launched in January 2009, was laid out in the white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008). Nakamoto's genius lay not in inventing new technical components from scratch, but in combining existing cryptographic concepts with a novel system of economic incentives to create a resilient, self-sustaining, and truly decentralized system (De Filippi et al., 2024). This synthesis rested on three key pillars.

First, the system relied on established principles of *public-key cryptography* for ownership and transaction validation. As in earlier proposals, ownership of the currency is proven by possession of a secret private key, which is used to create a digital signature that authorizes a transaction, while a corresponding public key serves as the address for receiving funds (Antonopoulos, 2014). Transactions are then chained together into a shared, chronological ledger using cryptographic hash functions, which ensure the integrity of the historical record (Narayanan et al., 2016).

Second, the entire system operates on a sophisticated *decentralized peer-to-peer (P2P) network architecture*. This design, which lacks any central server, central service, or hierarchy, is both a reflection and a technical foundation of the system's core characteristic: the decentralization of control (Antonopoulos, 2014; Narayanan et al., 2016). This architecture ensures that no single entity can dictate the rules or censor transactions.

The third and most crucial innovation was the use of *economic incentives* to solve the problem of network consensus. Nakamoto implemented a distributed computation system, the Proof-of-Work (PoW) algorithm, which required network participants (called "miners") to expend computational energy to solve a difficult but arbitrary puzzle in order to propose a new block of transactions (Nakamoto, 2008). The miner who solved the puzzle was rewarded with a block of newly created bitcoins and any transaction fees. This PoW mechanism, combined with its financial rewards, formed a "cryptoeconomic" structure designed to align the rational self-interest of participants with the overall security of the network. It is more profitable for miners to "play by the rules" and honestly validate transactions to earn the reward than it is to attempt to defraud the system and waste the energy they expended (Parkin, 2020). This elegant synthesis finally solved the double-spending problem, the core weakness of all earlier digital cash proposals, without resorting to a trusted central authority (Antonopoulos, 2014).

2.4.3 Defining Blockchain as a New Architecture of Trust

The resulting technology, now generically referred to as the blockchain, functions as a revolutionary new architecture of trust (Werbach, 2018). It is frequently described as a "trust machine" or a "confidence machine" (De Filippi et al., 2020). The core feature of this architecture is its ability to create confidence through a system of "trustless trust" (De Filippi et al., 2024). This seemingly paradoxical concept denotes a fundamental shift away from placing social trust in fallible humans or institutions and toward placing technical trust in the predictable behavior of the technology itself (Finck, 2018).

This new form of trust is achieved through several interlocking mechanisms. First, the technology enables peer-to-peer electronic transactions without relying on a financial institution or any other trusted third party for verification. Second, the system establishes robust and shared expectations because the code is formulaic and carries a repeatable integrity, ensuring a deterministic computation that produces the same result every time (Nabben, 2021). Finally, confidence arises from the system's resilience, its reliability, and the immutability of the data recorded on the append-only ledger (De Filippi et al., 2024). Users can independently verify that transactions have occurred and will not be altered, gaining a powerful assurance that their assets are protected by the network itself. By ingeniously weaving together cryptographic proof and economic incentives, Bitcoin established a technology that could produce confidence without the need for traditional, institutionally-mediated trust.

2.4.4 Blockchain as a Synthesis of Philosophy, Economics, and Code

The emergence of blockchain technology represents more than a mere technical innovation; it marks the arrival of a new form of institutional technology. These novel architectures embed specific, often unstated, assumptions about human nature, social order, and economic coordination directly into their software. This unique characteristic enables analysis through the complementary lenses of political philosophy and economic governance theory. To view a protocol as just code is to miss its function as a constitution for a digital society. This new paradigm creates a fundamental and ongoing tension between designs rooted in deeply individualistic, trust-minimizing philosophies and the collective, cooperative goal of sustainably managing a shared digital resource. The governance models embedded in these protocols function as a new form of social contract, one that pits the pessimistic security-oriented assumptions of *Thomas Hobbes* against the aspirational, collectivist ideals of *Jean-Jacques Rousseau* (Reijers et al., 2021). Simultaneously, these systems must solve a classic economic problem of resource management, a challenge best understood through the framework pioneered by Nobel laureate *Elinor Ostrom*. The result is a complex socio-technical system that is neither a traditional state nor a pure market, but a new form of protocol-governed network.

2.4.4.1 *The Digital Social Contract: An Automated Sovereign vs. The Common Good*

From a philosophical standpoint, many foundational blockchain protocols are built upon a distinctly *Hobbesian* worldview. In his seminal work *Leviathan*, Thomas Hobbes envisioned a hypothetical "state of nature" where, without a common power to enforce rules, life would be a "war of every man against every man", an existence he described as "solitary, poor, nasty, brutish, and short" (Hobbes & Missner, 2016). He argued that rational, self-interested individuals would willingly surrender their natural freedom to an absolute sovereign authority in exchange for security and order. This sovereign, the Leviathan, would stand above all, impartially enforcing the laws that prevent society from descending into chaos.

Blockchain architecture mirrors this conception with remarkable fidelity. Emerging from *cypherpunk* and *crypto-anarchist* movements deeply distrustful of existing human institutions like governments and banks, these systems are predicated on the assumption that

participants will act opportunistically if given the chance. The solution is not to foster trust, but to eliminate its necessity. The protocol's code itself is designed to function as an "*automated Leviathan*." It is an incorruptible and impartial sovereign whose laws are written in deterministic software. The rules governing the network, from transaction validity to consensus, are enforced automatically and inexorably by a distributed network of computers. This automated enforcement mechanism is the system's absolute authority, replacing interpersonal trust with what is often termed "*cryptographic proof*." Every participant, regardless of their identity or power in the outside world, is subject to the same immutable rules. The protocol, like Hobbes's Leviathan, is the ultimate arbiter, created to impose order and prevent the digital "war" of double-spends and fraudulent transactions.

This Hobbesian design, however, stands in stark contrast to the *Rousseauian aspiration for legitimate self-governance*. Jean-Jacques Rousseau offered a different vision of the social contract. For him, the goal was not to surrender freedom for security but to achieve a higher form of liberty through collective self-rule. Central to his theory is the critical distinction between the "*will of all*" (*volonté de tous*) and the "*general will*" (*volonté générale*) (Rousseau, 1913). The "will of all" is merely the sum of each individual's private, self-interested desires, an aggregation of particular interests. The "general will," by contrast, is the collective will of the citizenry that aims exclusively at the common good. A legitimate state, for Rousseau, is one that allows this general will to guide its actions.

This profound philosophical tension is mirrored directly in the governance challenges of blockchain technology. The most common form of on-chain governance is token-weighted voting, where decision-making power is proportional to the number of governance tokens a participant holds. This mechanism is a highly effective and quantifiable expression of the "will of all," as it efficiently aggregates the economic self-interest of token holders. This raises the fundamental Rousseauian dilemma: can such a system ever truly arrive at the "general will," the set of decisions that promotes the long-term health, security, and decentralization of the network? Or is it destined to be captured by the will of the largest token holders, leading to *plutocracy*? The persistent problem of "whales" (large stakeholders) dominating DAO votes demonstrates this conflict, where the interests of a wealthy minority can override the perceived common good of the broader community. This highlights the deep tension between a system designed around capital-weighted individualism and the democratic ideal of legitimate, collective self-rule.

2.4.4.2 Economics: Governing the Digital Commons

From the economics perspective, the work of *Elinor Ostrom* on the governance of common-pool resources offers a practical and empirically grounded framework (Ostrom, 1990). A public blockchain can be understood as a quintessential, albeit novel, form of a "*digital commons*" (Rozas et al., 2021). A common-pool resource is defined by two key characteristics: it is difficult to exclude beneficiaries (non-excludable), and its use by one person subtracts from the ability of others to use it (rivalrous). The shared resource in a blockchain is not a physical pasture but a complex of digital assets: the integrity of the distributed ledger, the security of the consensus mechanism, and the finite transactional capacity (block space) of the network. Without effective

governance, this digital commons is vulnerable to a "*tragedy of the commons*," where rational but uncoordinated individual actions could degrade the network's value for everyone.

Contrary to the pessimistic predictions of such a tragedy, Ostrom's Nobel Prize-winning research demonstrated that communities worldwide have successfully managed shared resources for centuries without top-down government control or privatization. This work identified a set of design principles common to long-enduring, self-governing institutions. Blockchain protocols can be seen as an automated, code-based implementation of these principles. The system's "*cryptoeconomics*", the use of cryptography and economic incentives to secure the network, maps remarkably well onto Ostrom's framework. For instance, Ostrom's principle of *monitoring* is achieved on a global scale through the public and transparent nature of the ledger, which allows anyone to audit the system's state and participants' behavior. The principle of *graduated sanctions* is enforced automatically through mechanisms like "slashing" in Proof-of-Stake systems, where validators who act maliciously have their staked capital programmatically confiscated. The *rules* of the commons are clearly defined and enforced by the protocol itself.

However, a profound paradox lies at the heart of this application. Ostrom's research focused almost exclusively on small-to-medium-scale, local commons where participants often knew each other, shared a long-term future, and relied heavily on social capital, trust, reputation, and community norms, for enforcement. Public blockchains are the complete opposite: they are large-scale, global, and pseudonymous networks built for a low-trust environment of strangers. The resolution to this paradox is that blockchain protocols do not directly implement Ostrom's principles as observed in traditional commons. Instead, they use cryptoeconomics to *synthetically replicate* the conditions that foster cooperation. The protocol's automated system of rewards (e.g., block rewards) and punishments creates a purely game-theoretic environment where it becomes economically rational for self-interested, anonymous actors to cooperate. In this model, explicit economic incentives serve as a powerful substitute for the social capital that was central to Ostrom's findings.

Building on these historical developments and conceptual perspectives, the next step is to delve into the internal mechanics of blockchain technology itself, clarifying how its underlying architecture operates in practice and how these technical realities correspond to (and often complicate) the ideological and theoretical visions that inspired its creation.

2.5 The Technical Apparatus of a Trust Machine

The blockchain technology first realized by the Bitcoin protocol is, at its foundation, an algorithmic architecture that represents a significant breakthrough in distributed computing. Its resilience and security are not derived from a single novel technology but from the masterful combination of several existing components, including peer-to-peer networking, public-key cryptography, and a consensus mechanism, into a system that produces a resilient and tamper-resistant ledger. To understand the philosophical and political implications of this technology, it is first necessary to grasp the mechanics of how this "trust machine" operates.

2.5.1 The Data Structure: Blocks, Hashes, and the Chain

The blockchain is, as its name suggests, an ordered, back-linked list of blocks of transactions (Antonopoulos, 2014). Transactions, which are data structures that encode the transfer of value between participants, are broadcast across the peer-to-peer network and collected into a temporary pool of unconfirmed transactions known as the "mempool" (Antonopoulos, 2014). At regular intervals, roughly every ten minutes in the Bitcoin protocol, network participants known as miners collect a group of these transactions and bundle them together to form a new block (Parkin, 2020). A block is essentially a container data structure, composed of a header containing metadata and a list of the transactions it confirms (Antonopoulos, 2014).

Within each block, all the included transactions are summarized into a single digital fingerprint using a data structure called a Merkle tree (Werbach, 2018). This is achieved by recursively hashing pairs of transaction data until only a single hash remains, a value known as the Merkle root (Antonopoulos, 2014). This 32-byte Merkle root, which acts as a unique summary of every transaction in the block, is then included in the block header. This structure is highly efficient, as it allows for the verification of a specific transaction's inclusion in a block without needing to download and process the entire block's contents (Antonopoulos, 2014; Narayanan et al., 2016). A user only needs the transaction data and the handful of hashes that form the "Merkle path" connecting it back to the Merkle root in the header to prove its validity.

The security and immutability of the entire chain hinge on the application of cryptographic hash functions. Bitcoin uses the SHA-256 algorithm, which is a mathematical one-way function that takes an input of any length (such as the entire data of a block) and produces a fixed-length output, or hash (Biondi Santi & Vespri, 2020; Gilbert & Handschuh, 2003). A crucial property of this function is the "avalanche effect": even a minuscule change to the input data will produce a radically different output hash, making the result impossible to predict or reverse-engineer (Gilbert & Handschuh, 2003). The key to the blockchain's structure is that each new block's header includes the hash of the *previous* block in the chain (Antonopoulos, 2014). This creates an unbreakable cryptographic link that chains every block, and by extension every transaction, back to the very beginning of the ledger (Magnuson, 2020). If an attacker were to attempt to modify a transaction in a past block, the hash of that block would change. This change would, in turn, invalidate the "previous block hash" field in the subsequent block, creating a cascade effect that would require the attacker to recalculate the proof-of-work for the altered block and *all* subsequent blocks in the chain (Antonopoulos, 2014). This makes the chain's deep history exceptionally resistant to tampering, creating a functionally immutable and append-only ledger where data can be added but not retroactively altered (Cappiello & Carullo, 2021; Finck, 2018). The entire chain begins with the "genesis block," which is statically encoded into the software of every node and serves as the secure, unalterable root of trust (Antonopoulos, 2014).

2.5.2 Cryptographic Sovereignty: Keys, Wallets, and Ownership

Ownership and control over digital assets on the blockchain are secured not by a centralized administrator or account system, but entirely by asymmetric cryptography. Every user utilizes a key pair composed of a private (secret) key and a public key. The private key is a randomly chosen large number that must remain secret at all costs, as it is the sole instrument of control over any associated funds. The public key is mathematically derived from the private key via a one-way cryptographic function, meaning reversing the procedure to get the private key from the public one is almost computationally impossible.

The public key is used to generate an address, which serves as the public identifier for receiving funds on the network (Parkin, 2020). To spend those funds, the owner must use their private key to create a digital signature for the transaction. This signature serves two purposes: it proves ownership of the private key without revealing the key itself, and it authorizes the specific transaction, ensuring it cannot be altered after it has been signed (De Filippi et al., 2024). Anyone on the network can then use the sender's public key to verify the signature's authenticity, confirming that the transaction was authorized by the true owner of the funds (De Filippi et al., 2024).

A user's private and public keys are managed by a piece of software known as a wallet (Antonopoulos, 2014). A common misconception is that wallets "hold" or "store" cryptocurrency. In reality, the coins exist only as records on the globally shared blockchain ledger. A wallet is simply a data structure or software application that holds and manages the private keys required to authorize transactions and "unlock" the right to spend those coins (Antonopoulos, 2014). This system of self-custody places the full responsibility for security on the individual user, a principle captured by the common aphorism in the cryptocurrency community: "not your keys, not your coins."

2.5.3 The Peer-to-Peer Architecture: Resilience and Propagation

The data structure of the blockchain is supported and maintained by a peer-to-peer (P2P) network architecture built on top of the internet. The network has a "flat" topology, meaning that the computers, or nodes, that participate are considered equals, with no central server or privileged administrator to coordinate their activity (Antonopoulos, 2014; Parkin, 2020). This decentralized structure is a direct technical implementation of the system's core political ideology, designed to eliminate single points of control. The resilience of the network is a direct result of this architecture combined with massive data replication. Every full node running the protocol maintains its own complete copy of the digital ledger. This shared, redundant maintenance ensures a remarkable degree of robustness, as there is no singular point of failure for an attacker to target or for a technical fault to cripple the system (Finck, 2018). So long as even a single computer in the world maintains a valid copy of the blockchain, the network's history can be fully restored (De Filippi & Wright, 2018).

When a user initiates a transaction, it is broadcast to all neighboring nodes to which it is connected. These nodes then validate the transaction and broadcast it to their neighbors, and so on, in a process known as "flooding" (Antonopoulos, 2014; Parkin, 2020). This exponential propagation ensures

that within seconds, the transaction has reached nearly every connected node across the globe. Because the network lacks a central gatekeeper or intermediary, it is designed to be censorship-resistant. There is no single entity with the authority to block a valid transaction from being broadcast and eventually included in the ledger, a feature that is fundamental to the system's political objectives (Cappiello & Carullo, 2021).

2.5.4 The Consensus Mechanism: Forging Agreement in a Distributed System

While the P2P network provides a means for communication, the most difficult challenge in any decentralized system is ensuring that all participants agree on a single, authoritative version of the truth. Consensus mechanisms are the protocols that ensure all geographically distributed nodes remain synchronized and agree on which transactions are legitimate and in what order they should be added to the blockchain (Finck, 2018). In designing Bitcoin, Satoshi Nakamoto provided an elegant solution to the decades-old computer science challenge known as the Byzantine Generals' Problem, which explores how a group of actors can reach a reliable agreement even if some participants are untrustworthy (Antonopoulos, 2014).

Bitcoin's solution is a consensus mechanism called Proof-of-Work (PoW), a computationally intensive process often referred to as "mining." In this system, miners compete to solve a difficult mathematical puzzle. Specifically, they must find a random number, called a "nonce," which, when combined with the data in the proposed block and the hash of the previous block, produces a new hash that meets a predetermined difficulty target, such as starting with a specific number of zeros (Biondi Santi & Vespri, 2020; Day, 2018). Because cryptographic hash functions are one-way, this puzzle cannot be solved through clever mathematics; it must be solved by brute force, with miners using powerful hardware to guess trillions of nonces per second until one of them finds a valid solution (Narayanan et al., 2016). The computational difficulty of this puzzle is automatically adjusted by the protocol to ensure that, on average, a valid block is found and added to the chain roughly every ten minutes, regardless of how much computing power is added to the network (Antonopoulos, 2014).

This energy-intensive process is secured by a carefully calibrated system of economic incentives. The miner who successfully finds the winning hash earns the right to add their block to the chain and is rewarded with a combination of newly minted coins and all the transaction fees from the transactions included in that block (Biondi Santi & Vespri, 2020). This reward system links the economic self-interest of miners directly to the desired behavior of the network. Miners are incentivized to act honestly because the reward they receive for playing by the rules is greater than any potential profit from attempting to cheat, an act that would require them to waste the immense amount of energy expended to find the proof-of-work. If multiple valid blocks are found simultaneously, creating a temporary fork in the chain, the network resolves the ambiguity with a simple rule: nodes always follow the chain that represents the greatest cumulative Proof-of-Work effort, which is effectively the longest chain. This ensures that the network eventually converges back to a single, consensus-driven state (Antonopoulos, 2014).

The high energy consumption associated with PoW is a major and widely criticized limitation (Cappiello & Carullo, 2021). Consequently, numerous alternative consensus mechanisms have been developed. The most prominent alternative is Proof-of-Stake (PoS). In PoS systems, validators are selected to create new blocks not based on their computational power, but on the amount of the network's cryptocurrency they hold and are willing to "stake" as collateral (Antonopoulos, 2014). This drastically reduces energy expenditure. Validators who fail to act honestly risk having their staked collateral "slashed" or destroyed, creating a financial disincentive for malicious behavior. The Ethereum blockchain, one of the largest in the world, has notably transitioned from PoW to a PoS system. Other approaches, such as Delegated Proof-of-Stake, which relies on token holders voting for representatives, are also in use (Parkin, 2020).

Ultimately, the combination of cryptographic assurance, decentralized architecture, and economic incentives creates a system where trust is shifted away from centralized human or institutional third parties and placed in the immutable rules of the software protocol itself (Cappiello & Carullo, 2021). This is why blockchain technology is often described as a "confidence machine" or a system of "trustless trust" (De Filippi et al., 2020; Werbach, 2018). This confidence is rooted in deterministic computation, where code executes in a formal, unambiguous way that always produces the same outcome. Users gain assurance from the system's resilience, reliability, and the immutability of its data, establishing shared expectations that transactions will be unambiguously ordered and correctly executed without reliance on fallible human intermediaries (De Filippi et al., 2024).

2.6 A Critical Analysis

Blockchain technology, first instantiated by the Bitcoin protocol, is widely regarded as more than a mere technical innovation; it is framed as a philosophical statement on how trust, power, and organization should operate in the digital age (Swan & De Filippi, 2017). It is the culmination of the techno-decentralist ideology, a mission to democratize societies by eliminating centralized points of control in economic systems (Parkin, 2020). Having detailed the historical origins and technical mechanics of this technology, it is now possible to critically examine its core philosophical claims and assess the significant gap between its visionary potential and its material realities.

A foundational claim of blockchain proponents, derived directly from the cypherpunk movement, is that the technology eliminates the need for trust in fallible human institutions. As Satoshi Nakamoto stated, the "root problem with conventional currency is all the trust that's required to make it work" (Nakamoto, 2008). Bitcoin was designed as a mechanism for electronic payments based on cryptographic proof "instead of trust," allowing parties to transact directly without a trusted third party. This led to the popularization of the term "trustless system" (Finck, 2018). However, a closer analysis reveals that trust is not eliminated, but rather transformed and displaced. Instead of relying on social or institutional trust in known third parties, participants are asked to place their trust in the technology itself, in the soundness of the cryptography, the integrity of the open-source protocols, and the reliability of the network as a whole (Cappiello & Carullo, 2021; Finck, 2018). Furthermore, confidence in the system ultimately depends on a web of

underlying trust relations among various human actors, including the core developers who write the code, the miners who secure the network, and the token holders who participate in governance (De Filippi et al., 2024).

This system vests its authority in a purportedly immutable code-based protocol that executes as planned regardless of the intent of the parties, giving rise to a system of rules often referred to as *lex cryptographica* (De Filippi & Wright, 2018). This creates a private regulatory framework enforced automatically by the network, operating outside or alongside existing jurisdictional laws. This ambition for a decentralized "rule of code" stands in stark contrast to the centralized "rule by code" of corporate platforms, as it is designed to be autonomously and impartially enforced by the technological infrastructure itself (Cappiello & Carullo, 2021).

Another core feature of this vision is the ideal of *immutability*, the exceptional difficulty of changing or deleting recorded information once consensus is reached, which is meant to ensure transaction finality and protect users from the arbitrary actions of a central authority (Antonopoulos, 2014). However, immutability is not an absolute technical property but rather a deeply held social norm and a matter of policy (De Filippi et al., 2024). This tension between code-driven absolutism and human agency was demonstrated dramatically by The DAO attack in 2016. When an attacker exploited a vulnerability in a smart contract on the Ethereum network to drain tens of millions of dollars' worth of funds, the community was faced with a choice: either uphold the principle of immutability and allow the theft to stand, or intervene. Ultimately, a majority of the community chose to execute a "hard fork", a contentious software upgrade, to reverse the transactions and recover the stolen funds. This event revealed that a sovereign human decision, reached through social consensus, could ultimately prevail over the technical finality of the code (DuPont, 2017).

The most potent critique of blockchain technology is that its feature of decentralization often obscures the ways in which power inevitably consolidates in new, and sometimes less accountable, forms (Schneider, 2019). Despite the decentralized design, power has consistently reconcentrated around several centralized bottlenecks or "obligatory passage points" within the network architecture. The economic incentives built into Proof-of-Work, for example, led to a hardware "arms race" that encouraged individual miners to coalesce into large, coordinated mining pools to achieve economies of scale and earn more predictable rewards (Magnuson, 2020; Finck, 2018). This consolidation centralizes the power to validate transactions and secure the network. At various points, a small handful of mining pools have controlled over 50 percent of the hashing power on both the Bitcoin and Ethereum networks, raising concerns about the risk of a "51% attack," where a majority actor could potentially rewrite transaction history or alter protocol rules (Eyal & Sirer, 2014; Finck, 2018).

Furthermore, governance systems that rely on a "one token, one vote" model often function not as a participatory democracy, but as a plutocracy, where power is distributed proportionally to economic share (Barbareau et al., 2022; Cappiello & Carullo, 2021). Given the stark concentration of wealth in most cryptocurrency ecosystems, where a few large holders or "whales" control a significant portion of the circulating supply, a very small number of individuals can exercise decisive influence over protocol changes (Ziolkowski et al., 2020b). Finally, considerable *de facto* power is concentrated at the software level in the hands of a select few core software developers.

These individuals, while often acting with the community's best interests at heart, function as an informal technocracy with immense influence over the protocol's maintenance and evolution, effectively acting as the legislators of the network (Parkin, 2020).

2.7 Conclusion: From Ideology to Infrastructure

The intellectual journey through the early visions of cyberspace, the enclosure of the digital commons, the rise of surveillance capitalism, and the cypherpunk counter-revolution reveals a multifaceted narrative of digital evolution, one propelled by the interplay between utopian aspirations and pragmatic technological innovation. Blockchain technology, first realized through Bitcoin, emerges as the culmination of decades of this dialectic between idealism and engineering (Barbrook & Cameron, 1996). Conceived in direct response to the systemic failures exposed by the 2008 global financial crisis, it sought to replace institutional trust with mathematical certainty and centralized governance with algorithmic coordination. In doing so, Satoshi Nakamoto's synthesis materialized the cypherpunk vision of a stateless, peer-to-peer monetary system, an experiment in redistributing power through cryptographic consensus and coded governance (Parkin, 2020).

This technological paradigm fundamentally reconfigures the architecture of trust, transforming confidence in human institutions into verifiable assurance in autonomous, immutable computation (De Filippi et al., 2020; Werbach, 2018). Yet, as this chapter has demonstrated, the dream of absolute decentralization remains elusive. Despite its emancipatory rhetoric, blockchain systems are not immune to the re-emergence of power asymmetries, social hierarchies, and new intermediaries hidden within the layers of protocol design, code maintenance, and token distribution. The technology thus exposes an enduring paradox: the pursuit of digital liberation through governance by code inevitably encounters the persistent realities of law, markets, and human behavior (Magnuson, 2020).

Having traced blockchain's ideological lineage, technical foundations, and philosophical contradictions, the inquiry now turns from origins to operations. The following chapters will examine blockchain not merely as a financial innovation but as a *governance technology*, a socio-technical system capable of re-shaping how authority, coordination, and accountability are structured. Chapter 2 will analyze its role in *public governance*, exploring how states and institutions experiment with blockchain-based solutions to enhance transparency, participation, and trust. Chapter 3 will shift to *private governance*, focusing on *Decentralized Autonomous Organizations (DAOs)* as the most transformative embodiment of blockchain's governance potential. Finally, Chapter 4 will confront the legal frontier, the evolving *regulatory landscape* that both constrains and enables blockchain's mainstream adoption, through a critical analysis of emerging DAO and corporate law frameworks. Together, these chapters aim to evaluate whether blockchain can truly deliver on its ideological promise: the creation of more transparent, accountable, and decentralized forms of governance in the digital age.

3 Chapter 2: Blockchain in Public Governance

3.1 Introduction and Research Context

This chapter investigates how blockchain technology is being adopted within public administration and evaluates whether it can meaningfully contribute to the ongoing transformation of state governance. Building directly on Chapter 1's ideological genealogy, it examines how a technology born from distrust in centralized institutions has become an option to influence those very institutions, state bureaucracies and administrative authorities. The significance of this tension cannot be overstated: blockchain emerged as an anti-statist project grounded in techno-decentralist ideals (De Filippi et al., 2024; Parkin, 2020), yet governments worldwide explore its integration to enhance transparency, accountability, and efficiency in public services (OECD, 2020; World Economic Forum, 2021).

Historically, public administration has evolved through several governance paradigms. Weberian bureaucracy emphasized legality, hierarchical authority, and rule-based neutrality (Weber, 1922). New Public Management later shifted focus toward market mechanisms, privatization, and efficiency (Hood, 1991). In recent decades, the growing complexity of interdependent societies has advanced New Public Governance (NPG), which prioritizes network-based coordination, collaboration across stakeholders, and participatory modes of legitimacy (Rhodes, 1996; Kjaer, 2011). Blockchain intersects with NPG by offering programmable transparency and trust infrastructures that can mediate interactions across organizations without centralized oversight (Berryhill et al., 2019; Caradonna, 2021).

Despite these promises, integration into the public sector is not straightforward. Many technical affordances, immutability, decentralization, “trustless” automation, introduce conceptual tensions with administrative law, democratic accountability, and proportionality requirements (Finck, 2018; G'sell & Martin-Bariteau, 2022). The technology's design reflects a presumption that trust must be minimized, yet public governance is inherently a trust-dependent, legitimacy-based institution. This chapter interrogates whether these normative foundations can be reconciled.

Whereas Chapter 1 revealed blockchain's ideological origins, and Chapter 3 will explore its radical private-sector governance instantiations in DAOs, the present chapter provides a crucial middle anchor: the public sector as the first domain where blockchain's institutional aspirations collide with the realities of law-bound governance.

3.1.1 Research Statement and Questions

This chapter critically examines whether blockchain can be meaningfully integrated into public administration in ways that enhance transparency, accountability, and institutional legitimacy, while remaining compatible with constitutional principles and the integrity of administrative law. Rather than assuming that blockchain inherently improves governance, the chapter interrogates

the normative and structural consequences of embedding administrative authority into technical systems. The analysis highlights that public sector governance depends upon discretion, proportionality, and contestability, qualities that may be strained by blockchain's rigidity and automation (Finck, 2018; Alston, 2020).

Accordingly, this chapter is driven by the following research questions, each directly tied to the analytical and empirical directions of the text:

1. How does blockchain's design logic, including decentralization, immutability, and transparency, align with or challenge the principles of public law such as legality, due process, privacy protection, and accountability?
2. To what extent can blockchain support the shift toward New Public Governance by enabling distributed coordination, administrative interoperability, and pluralistic oversight?
3. Can "trust-minimizing" technological infrastructures strengthen citizens' trust in public institutions, or do they introduce new forms of opacity, exclusion, and technical power asymmetry?
4. What governance risks arise when administrative authority is automated through smart contracts, particularly in relation to proportionality and rights-based safeguards?
5. What institutional lessons can be drawn from real-world public-sector blockchain deployments such as digital identity systems, land registries, and procurement oversight tools?

These questions position the public sector as a critical test environment: a domain where blockchain's governance promises must confront legal durability and democratic legitimacy, rather than purely technical feasibility.

3.1.2 Methodology

This chapter adopts a qualitative, interpretive research paradigm to investigate the complex interplay between public law, governance, and technology. The central research question how a decentralized technology is being integrated into the centralized constitutional state, cannot be adequately answered through quantitative methods, as it is not a question of *how much* or *how often*, but rather of *how* and *why*. It concerns the meaning-making processes, normative conflicts, and institutional adaptations that characterize the adoption of blockchain in the public sector. An interpretive approach is therefore essential, as it allows for a deep, contextualized understanding of this socially constructed phenomenon, recognizing that the technology's impact is not predetermined by its technical features but is shaped by the legal, political, and organizational environments into which it is introduced.

3.1.3 Research Design and Approach

The chapter is designed as a *comprehensive, multi-disciplinary, literature-based study* that employs a method of *thematic synthesis*. This approach is particularly well-suited for a rapidly evolving field where empirical data is largely documented in a disparate and varied body of texts rather than in structured datasets. The chapter aims to build theory by synthesizing existing knowledge from diverse fields to construct a coherent and novel argument about the "*governance paradox*." This involves a systematic process of identifying, analyzing, and integrating findings from a wide range of sources to develop a higher-order theoretical framework that explains the observed patterns of public sector blockchain adoption.

3.1.3.1 Data Collection: A Multi-Disciplinary Literature Review

The primary data for this chapter consists of a curated body of textual sources, selected to provide a holistic view of the research problem. The literature review was conducted systematically, employing keyword searches in major academic databases (e.g., JSTOR, Google Scholar, Scopus), legal databases (e.g., HeinOnline, Westlaw), and repositories for governmental and institutional publications (e.g., European Commission, World Bank). The sources were selected based on their relevance, the authority of the author or institution, peer-review status (for academic articles), and their citation frequency within the field.

The collected body of literature can be categorized into four main types:

1. **Doctrinal Legal and Jurisprudential Scholarship:** This includes law review articles, academic legal treatises, and scholarly books that analyze the foundational principles of public law, administrative law, constitutional theory, and the emerging field of "blockchain and law" This literature forms the basis for understanding the normative framework of the "Rule of Law."
2. **Public Administration and Governance Theory:** This includes academic literature on public sector innovation, digital transformation, and governance models, particularly the literature defining New Public Governance (NPG). These sources provide the theoretical lens for understanding the organizational and institutional context.
3. **Technical and Computer Science Literature:** While this is not a technical thesis, a review of foundational technical papers (including the original Bitcoin white paper), computer science articles, and explanatory texts was necessary to ensure an accurate and nuanced understanding of blockchain's core properties and their limitations.
4. **Grey Literature and Empirical Case Studies:** This crucial category provides the empirical grounding for the thesis. It includes a wide range of reports from governmental bodies, white papers from pilot projects, policy analyses from international organizations (such as the OECD, World Bank, and European Commission), and research from respected think tanks.

3.1.3.2 Method of Analysis: Thematic Synthesis

The analysis of the collected literature was conducted using a thematic synthesis approach, which involves a three-stage process:

1. **Free Line-by-Line Coding:** A thorough reading of all selected texts was undertaken to identify key concepts, arguments, findings, and examples. Initial codes were generated to capture the essence of these points (e.g., "legal uncertainty hinders adoption," "preference for permissioned chains").
2. **Organization into Descriptive Themes:** The initial codes were then grouped and organized into a hierarchical structure of related "descriptive themes." These themes represent the recurring patterns and issues identified across the literature, such as the consistent focus on incremental efficiency or the architectural compromises made to ensure GDPR compliance.
3. **Generation of Analytical Themes:** The final and most critical stage involved moving beyond description to interpretation. The descriptive themes were synthesized to generate higher-order "analytical themes" that form the core argument of the thesis. This involved interpreting the relationships *between* the themes to build the central concept of the "governance paradox" and the overarching narrative of institutional co-option and adaptation.

3.1.4 Contributions

This chapter contributes to the thesis and to the argument that blockchain in government is not merely a tool for administrative efficiency. Instead, it functions as a significant governance intervention that reshapes how authority is exercised, monitored, and legitimated. Consequently, as the chapter illustrates, applying blockchain in public governance requires careful consideration of issues spanning not only efficiency but also control, trust, law, and governance. The success of such applications, therefore, depends on this multitude of factors.

The chapter advances the historical narrative established in Chapter 1 by revealing how a technology rooted in anti-statist ideology is now being selectively integrated into state authority structures. Simultaneously, it establishes essential groundwork for Chapter 3 by showing that governance outcomes are fundamentally contingent upon institutional context: where the state may recentralize blockchain deployments, decentralized private organizations seek to operate *without* state scaffolding. Through this multi-layered analysis, the chapter clarifies the stakes of public-sector experimentation and why legal principles must remain central as blockchain evolves into a tool of public power.

3.1.5 Literature Review

The integration of blockchain technology into public administration exists at the nexus of several distinct and rapidly evolving fields of study. A comprehensive understanding of this phenomenon requires a multi-disciplinary approach, drawing insights from foundational legal and governance theory, the burgeoning scholarship on techno-legal systems, and the growing body of empirical

research on real-world implementations. The literature reveals a clear trajectory in thought, moving from early, speculative, and often utopian theories about the technology's potential to a more grounded, critical, and empirically-informed analysis of its practical application and inherent limitations.

The first essential body of literature provides the constitutional and administrative benchmark against which blockchain's disruptive claims must be measured. This scholarship establishes public governance not as a mere set of administrative processes, but as a normative framework grounded in centuries of legal and political philosophy designed to ensure the legitimate exercise of state power.

At the apex of this framework stands *the Rule of Law*, a principle articulated by scholars like Dicey (1885) and Bingham (2010) as the mechanism holding all institutions accountable to law. This is intrinsically linked to the principle of *Legality*, which holds that public authorities can only act where they have explicit legal authorization.

Further scholarship details the procedural safeguards that protect individuals from arbitrary state action. These include *Due Process*, the guarantee of fairness ensuring notice and a meaningful opportunity to be heard, and *Proportionality*, a cornerstone of administrative law dictating that any state action infringing on rights must be suitable, necessary, and proportionate to its public goal (Barak & Kalir, 2012).

This body of work also traces the evolution of administrative models. It contrasts the classical, hierarchical *Weberian bureaucracy* and the market-driven *New Public Management (NPM)* with the contemporary paradigm of *New Public Governance (NPG)* (Osborne, 2006). NPG defines governance as a networked, collaborative, and multi-actor framework (Osborne, 2006), providing the modern context into which blockchain technology is being introduced (Brinkmann, 2021).

In direct opposition to this state-centric literature stands a vibrant body of scholarship examining the technology itself and its ideological underpinnings.

The foundational literature details the initial techno-utopian or techno-libertarian vision for blockchain, which was highly ideological and explicitly anti-statist (Atzori, 2017). This work frames the state as an "illegitimate... depository of power" (Atzori, 2017) and posits that blockchain enables civil society to replace traditional state functions with distributed consensus.

The core promise was to establish "trust-by-computation" (Antonopoulos, 2014), thereby obviating the need for trusted third-party intermediaries like governments (Nakamoto, 2008). This gave rise to the theoretical concept of *Lex Cryptographia*, a new legal order where rules embedded in code function as inviolable law (Becker, 2022), competing with or replacing traditional legal frameworks (De Filippi & Wright, 2018).

However, a significant and growing counter-literature offers a critical assessment of this vision, arguing it represents an overstatement of the technology's political potential (Atzori, 2017; Park et al., 2021) and risks promoting anti-political instruments (Atzori, 2017; Paquet & Wilson, 2015). This critical scholarship challenges the core claim of "disintermediation" (Nakamoto, 2008), demonstrating that in practice, blockchain creates *new forms of intermediation* (A. Zwitter

& Hazenberg, 2020). Power does not evaporate but morphs into new centralized forms, such as the influence wielded by code developers and wealthy token holders, who can become new oligarchies (Atzori, 2017; Barbereau et al., 2023). This literature reframes blockchain not as a "trustless" technology but as a "*confidence machine*" (De Filippi et al., 2020), arguing that confidence is ultimately built upon an external layer of human trust in the network's governance (M. Becker & Bodó, 2021a; De Filippi et al., 2020).

The third major body of literature moves from theory to practice, providing empirical analysis of real-world blockchain implementations in the public sector.

A consistent finding across these studies is that governments overwhelmingly prefer *permissioned (private or hybrid) blockchains* over their public, permissionless counterparts (Dib et al., 2018; Lianos, 2019). This architectural choice is explained as a pragmatic necessity, driven by the public sector's need for clearer governance, higher efficiency, and the ability to ensure compliance with legal frameworks, especially data protection regulations (Goossens, 2021; Reddick et al., 2021).

This scholarship provides a typology of governmental pilot projects, documenting initiatives in areas like *identity management, public records, financial management, and democratic processes*. These studies offer concrete evidence of potential benefits, such as the dramatic efficiency gains seen in Georgia's land title registry, where registration became 400 times faster and costs were reduced by over 90% (Bustamante et al., 2022; Cagigas et al., 2021).

Despite these benefits, this same body of work extensively documents the *decisive bottlenecks* and systemic risks that impede widespread adoption. This literature repeatedly confirms that the most significant barriers are *not technical* but are rooted in *governance, legal clarity, and organizational readiness* (Tan et al., 2022). Regulatory uncertainty is consistently identified as the most significant risk, often preventing successful pilots from becoming operational (Cagigas et al., 2021; Bosch et al., 2022).

A critical sub-field within this empirical literature is the analysis of the conflict between blockchain and the *General Data Protection Regulation (GDPR)*. Scholars have detailed the fundamental tension between the technology's core feature of *immutability* and the data subject's *rights to erasure and rectification* under the GDPR (Finck, 2018; Reddick et al., 2021). This literature is crucial for understanding the design patterns that have emerged in response, such as storing personal data off-chain while only cryptographic references are stored on the ledger (Berryhill et al., 2018). These studies show how legal frameworks act as a hard constraint, actively shaping the technology's design and implementation (Finck, 2018).

3.1.6 Chapter Structure and Plan

The first analytical section interrogates blockchain's compatibility with the principles that anchor modern administrative law, legality, due process, accountability, privacy, and proportionality. These principles embody the legal expression of democratic legitimacy, and thus they form the conceptual boundary within which any technological reform of governance must operate.

The discussion explores how blockchain's core affordances, decentralization, immutability, transparency, and automation, simultaneously enable and constrain compliance with these public-law standards. For instance, the immutability of blockchain records may secure evidentiary reliability but undermines administrative corrigibility, the state's obligation to correct or revoke unlawful acts (Finck, 2018). Likewise, decentralization diffuses operational control but complicates accountability chains, challenging the principle that every administrative act must have a legally identifiable author (Allen, 2020).

This section thereby provides the normative foundation for the chapter, establishing why technology cannot be evaluated purely through the lenses of efficiency or cost-reduction. Instead, it must be assessed in relation to the juridical fabric of the administrative state. It directly addresses *Research Question 1*, clarifying where blockchain aligns with and where it diverges from the obligations of legality and rights protection.

The second section situates blockchain within the broader theoretical context of New Public Governance (NPG). NPG emphasizes collaborative, network-based coordination among governmental agencies, private organizations, and civic actors (Rhodes, 1996; Kjaer, 2011). Blockchain, with its distributed verification and consensus protocols, appears conceptually aligned with this model: it can mediate inter-organizational cooperation through shared ledgers that reduce transaction costs and information asymmetries (Berryhill et al., 2019).

The analysis, however, interrogates this alignment critically. Blockchain's decentralization may support horizontal coordination but can also ossify power asymmetries if control over technical parameters, such as node participation or protocol updates, remains confined to small expert groups or private contractors (De Filippi & Wright, 2018; World Economic Forum, 2022). The section thus asks whether blockchain contributes to genuine pluralistic oversight or merely recentralizes authority under a new, technocratic form.

By integrating governance theory with socio-technical analysis, this section engages *Research Question 2* and *Research Question 3*, examining whether blockchain can facilitate cooperative legitimacy and citizen trust without eroding the accountability and transparency standards of democratic governance. It also deepens the theoretical transition from Chapter 1's discussion of decentralization as ideology toward its institutional manifestation in state systems.

The third section turns to the operational dimension of blockchain in public governance, the automation of administrative functions through smart contracts and algorithmic enforcement. Here, blockchain is examined as a medium of "rule-by-code," in which legal norms are transformed into executable logic (Goossens, 2021). This process promises predictable, impartial decision-making but also risks removing the interpretive flexibility essential to proportionality and justice (Alston, 2020).

The section analyses how automation redefines the traditional balance between rule application and administrative discretion. When smart contracts automatically execute welfare disbursements or procurement conditions, they eliminate the temporal and procedural spaces in which public officials typically exercise judgment and contextual reasoning. The discussion draws on examples

such as automated subsidy allocation and digital licensing platforms to highlight the paradox of efficiency: increased reliability may coexist with diminished fairness and responsiveness.

This part engages *Research Question 4* by assessing whether algorithmic enforcement enhances the legality of administrative acts or instead introduces new forms of rigidity and error that escape existing accountability frameworks. It also links back to Chapter 1's exploration of "code as law," demonstrating how this concept materializes concretely within governmental infrastructures.

The fourth section grounds the theoretical analysis in empirical observation by examining concrete governmental experiments with blockchain technologies. These cases, including digital identity management systems and blockchain-based land registries illustrate how the technology operates under real institutional constraints. For instance, Estonia's use of blockchain for data integrity in state registries and the Republic of Georgia's blockchain-based land-titling system exemplify implementations that reinforce record authenticity and citizen auditability (OECD, 2020). Conversely, pilot programs in welfare administration and public-procurement monitoring reveal limitations in scalability, data governance, and compliance with privacy regulations.

Through these cases, the chapter assesses how governments reinterpret blockchain's decentralization to suit bureaucratic logics of control and verification. Rather than creating "governance without government," most deployments reveal "distributed centralization", where transparency and immutability strengthen the surveillance and auditing capacities of existing authorities.

This section therefore answers *Research Question 5*, distilling institutional lessons from practical applications and demonstrating how blockchain's political economy shifts when embedded within sovereign systems. It provides empirical grounding to the earlier theoretical claims, ensuring that normative analysis remains anchored in observable practice.

The final section synthesizes insights from the preceding analyses into an overarching assessment of blockchain's role in public governance. It argues that blockchain functions less as a revolutionary force dismantling bureaucratic hierarchies than as an evolutionary technology that can reinforce, recalibrate, or marginally transform them depending on its institutional embedding. When used to improve auditability, inter-agency cooperation, and record integrity, blockchain can augment the legitimacy of public administration. When used for rigid automation or surveillance, it risks eroding fundamental administrative values.

This synthesis reaffirms that the integration of blockchain into public governance is inherently dialectical, it reveals both the resilience of legal norms and the persistent drive toward algorithmic rationalization. The section thus prepares the conceptual bridge to *Chapter 3*, where the thesis turns from blockchain *within* the state to blockchain *beyond* the state. The next chapter examines Decentralized Autonomous Organizations (DAOs) as laboratories for entirely post-bureaucratic governance, where rules are not constrained by administrative law but are encoded directly into the operational architecture of digital communities.

By contrasting the state's partial, legality-bound adoption of blockchain with DAOs' full algorithmic autonomy, the transition clarifies the continuum explored across the thesis: from

ideological decentralization (Chapter 1) through institutional adaptation (Chapter 2) to structural experimentation (Chapter 3). Together, these chapters trace blockchain's metamorphosis from a political ideal into a concrete apparatus of governance, both public and private, revealing the persistent tension between autonomy, accountability, and authority in the digital age.

3.2 Public Governance as a Normative Constitutional Framework

This chapter will focus on the potential, impact and the reality of blockchain technology in public governance. However, before any meaningful assessment of a technology's impact on the state can be undertaken, it is essential to first define, with precision, the normative environment into which it is being introduced. In the context of a rigorous legal-administrative analysis, *public governance* is not merely a synonym for government administration or a description of policy implementation; it is a comprehensive and deeply entrenched normative framework, built upon centuries of accumulated legal and political philosophy. This framework encompasses the vast web of formal and informal norms, institutions, and processes through which public authority is exercised. Its ultimate purpose, however, is not simply to manage public affairs efficiently, but to ensure that the coercive power of the state is wielded legitimately, fairly, and effectively. It represents the complex, dynamic interplay between the state, the market, and civil society in the collective pursuit of societal goals, an entire system anchored by an unwavering commitment to a set of foundational principles rooted in public law.

These principles, including the rule of law, legality, due process, proportionality, the separation of powers, transparency, and accountability, are not abstract or distant ideals to be admired from afar. They are concrete, operational requirements that actively shape the architecture of public institutions and serve as the primary constraints on the exercise of arbitrary power. As governments around the world increasingly turn to complex digital infrastructures and automated systems to perform their most critical functions, these enduring norms take on a new and urgent significance. They serve as both the critical design constraints that must guide the development of any public-sector technology and the essential, non-negotiable criteria against which the legitimacy of what might be termed "governance by algorithm" must be evaluated.

At the very apex of this normative structure stands the *rule of law*, the bedrock principle that all persons and all institutions, most critically including the state itself, are accountable to laws that are publicly promulgated, equally enforced, and independently adjudicated (Dicey & Wade, 1939; Nai, n.d.). This principle is the fundamental assertion that governmental authority is neither absolute nor arbitrary but is, in fact, derived from and strictly limited by a higher legal order. The tenets of the rule of law, as articulated by legal scholars, are both procedural and substantive. They demand that laws be prospective rather than retroactive, that they be open and clear to the citizens they govern, and that they remain relatively stable over time to allow individuals and organizations to plan their affairs with a degree of certainty. Furthermore, the creation of specific laws must be guided by open, stable, clear, and general rules to ensure predictability and fairness in the legislative process itself. Critically, this principle requires that the institutional independence of the judiciary be fiercely guaranteed, and that the courts possess the ultimate power to review the

implementation of laws to ensure their conformity with higher legal and constitutional standards, acting as the final guarantor of the entire framework (Raz, 2009).

Intrinsically linked to the rule of law, and flowing directly from it, is the principle of *legality*. This principle holds that public authorities may only act where they have explicit legal authorization to do so (European Commission, n.d.). It is the operational mechanism that translates the abstract limits of the rule of law into the daily functions of the state. Every single action undertaken by a government agency, from the collection of taxes to the implementation of a social benefit program, must be grounded in a specific and identifiable legal mandate granted by a legislature. This foundational requirement serves as the primary bulwark against administrative overreach, preventing officials from acting on personal whim, political expediency, or any authority other than that which has been lawfully prescribed to them. In the digital context, the principle of legality assumes an even greater, more critical significance. It demands that any automated system making decisions that have a legal effect on individuals, such as determining eligibility for a benefit, assigning a risk score, or enforcing a penalty, must operate on a clear and explicit legal basis. Therefore, the deployment of a specific technology like blockchain for a public function is not a mere technical or administrative choice to be made by an agency. It is a profound legal and political act that must be explicitly authorized by a law that defines its scope, its purpose, and its limitations, thereby ensuring that the technological architecture, no matter how innovative or efficient, remains firmly subordinate to the constitutional framework it is meant to serve.

Complementing the foundational principles of the rule of law and legality are the guarantees of due process and proportionality, which ensure fairness in the state's interactions with individuals. *Due process* is a fundamental commitment in republican legal systems that the state must respect all legal rights owed to a person before depriving them of life, liberty, or property (Linde, 1975). This principle contains two core components. The first, *procedural due process*, requires that government must follow fair and established procedures, ensuring that individuals receive advance notice of any action that may affect their rights and, critically, a meaningful chance to present their case before an impartial decision-maker (Citron, 2007). This includes the right to be informed of allegations, the right to present evidence, and the right to a decision from a neutral arbiter, all of which protect against arbitrary or unjust governmental actions. The second component, *substantive due process*, extends beyond procedural fairness to protect certain fundamental rights from government interference altogether, regardless of the procedures followed. It asks not *how* a law is enforced, but *whether* the government has an adequate reason to regulate or restrict certain rights in the first place.

When government operations are digitalized, these long-standing requirements of due process persist and must be actively translated into system design. An individual subject to a decision made by a blockchain-based system, such as the automated enforcement of a rule by a smart contract, must be given meaningful notice about how that decision was reached, including the logic embedded within the system, and afforded a genuine opportunity for review and appeal that typically involves human intervention (Citron, 2007). This is reinforced by the principle of *proportionality*, a cornerstone of administrative law, particularly within European legal traditions (Marsch & Tünsmeier, 2015). Proportionality dictates that any measure taken by a public authority that infringes upon an individual's rights must be a justifiable and appropriate means of achieving a legitimate public goal. This involves a rigorous three-part test: the measure

must be *suitable* to achieve the objective, it must be *necessary* in that no less intrusive means is available, and its benefits must outweigh the harm it causes to the affected right or interest, making it *proportionate in the narrow sense* (Barak & Kalir, 2012). For example, a blockchain system implemented for a public function must be evaluated not only for its effectiveness but also for whether its impact on fundamental rights, such as privacy or the right to be forgotten, is a necessary intrusion and whether that intrusion is excessive relative to the administrative or security gains it provides.

3.2.1 A Power Shift

In direct opposition to this state-centric, constitutionally-bound vision of governance stands the ideological framework that originally animated blockchain technology. The initial vision for blockchain governance was not one of administrative reform but of radical, anti-statist transformation (Atzori, 2017). Techno-libertarians and crypto-anarchists believed that the technology enabled a new mode of social organization capable of replacing traditional state functions, coercion, and hierarchies with mechanisms of distributed consensus (Atzori, 2017). This architectural shift gave rise to the concept of *Lex Cryptographia*, a new legal order where rules established by code function as law, competing with or even displacing traditional public law frameworks (K. Becker, 2022). This emerging framework of rules is defined by the underlying blockchain protocol and automatically enforced by the distributed network of participants, thereby challenging the authority and sovereignty of the traditional nation-state (Wright, 2021).

The central expectation of this paradigm was that power would shift from legal rules administered by government authorities to code-based rules and protocols governed by decentralized networks (Clifton & Pal, 2022; Pollicino & De Gregorio, 2021; Swan & De Filippi, 2017). This argument, famously encapsulated in the phrase “Code is Law,” posits that the architecture of cyberspace, the software and protocols structuring the digital environment, is itself a powerful, self-enforcing form of regulation (Lessig, 2009). Unlike legal rules, which can be debated, interpreted, or disobeyed, code is often designed to be absolute. It does not persuade; it compels. An algorithm that automatically disqualifies a benefit application based on predefined criteria does not offer a warning or an opportunity for appeal; it simply executes the outcome.

In this shift, blockchain technology introduced several perceived advantages: *transparency*, as every transaction is recorded on an immutable public ledger; *security*, through cryptographic verification that resists tampering or unauthorized alteration; *efficiency*, by automating enforcement through smart contracts that reduce administrative overhead; and *resilience*, as decentralized consensus mechanisms eliminate single points of failure and reduce dependence on centralized intermediaries. These features collectively embody the hope that technological systems could deliver fairer, more reliable, and more trustworthy governance than traditional bureaucratic or institutional models.

However, scholarly analysis and practical experience have quickly demonstrated that this utopian vision was often an overstatement of the technology’s political potential and that proposals based on such technological determinism are highly susceptible to promoting anti-political instruments

or reducing complex political decision-making to mere market logic (Atzori, 2017; Paquet & Wilson, 2015). The core claim of "disintermediation", that blockchain eliminates the middleman (Nakamoto, 2008), is frequently challenged by the realities of real-world application. The notion of "*authority floating freely*" in a decentralized network has proven to be deceptive, as power does not simply vanish; rather, it morphs and reconstitutes itself into new, often subtle or hidden, centralized forms (Atzori, 2017). In practice, blockchain implementation creates *new forms of governance structures*. Instead of displacing public institutions, the technology often acts as a complementary or partially substitutable solution for specific administrative functions (Alessie et al., 2019). Regarding that, the first wave of public sector applications was not characterized by open, permissionless systems but by numerous *permissioned, purpose-built platforms* run by consortia or central institutions, which involve sharing control and collaborating among a select group of public and private actors (Dib et al., 2018; Lianos, 2019).

Furthermore, a new class of powerful intermediaries has emerged in the form of *code developers* and technical elites, or "technopreneurs." These actors, by virtue of their specialized skills, gain a privileged position as the architects of the new systems, effectively becoming policymakers and potentially leading to the formation of new *oligarchies* within the distributed ecosystem (Atzori, 2017; Barbereau et al., 2023). This assertion of authority through technical design constitutes, as Bruno Latour noted, "politics pursued by other means" (Latour, 1988). The persistence of these new intermediaries means that the legitimacy of their actions and their code-based procedures must be rigorously assessed against fundamental public values and the rule of law (De Filippi et al., 2020; Pollicino & De Gregorio, 2021). Ultimately, a more grounded conclusion can be reached: blockchain-based public governance should be seen primarily as *a novel governance technology* offering technical and operational improvements, but not as *a whole package replacement of current practices*.

3.2.2 The Central Tension: Reconciling Blockchain with Constitutional Law

The integration of digital infrastructures into public administration generates a profound and enduring tension between the logic of technology and the principles of constitutional governance. This friction manifests through several interrelated dialectics that define the challenge of positioning blockchain within the modern state. The first concerns the conflict between the *immutability* of code, the algorithmically enforced, self-executing rules by *smart contracts* that underpin blockchain systems, and the law's foundational values of contestability, flexibility, and discretionary justice. The second tension arises from *the decentralized network architecture* of blockchain, which disrupts traditional hierarchical structures of authority and complicates the allocation of legal responsibility and public accountability. The third centers on blockchain's radical *transparency*, which, while enhancing openness and traceability, directly collides with the rights to rectification and erasure enshrined in the GDPR. Moreover, decentralization itself can exacerbate accountability gaps, as decision-making becomes diffused across anonymous or pseudonymous participants. Navigating these tensions, between code and law, decentralization and accountability, transparency and privacy, is the central challenge for any administration seeking to harness blockchain's advantages while safeguarding the core principles of democratic governance and the rule of law.

The first and most significant conflict arises from the clash between blockchain's algorithmic immutability and the dynamic, contestable nature of public law. Blockchain systems, particularly those that utilize smart contracts, are designed to apply encoded rules with maximum efficiency and finality. Their core strength is *immutability* and *self-enforcing smart contracts*, properties that provide a secure, tamper-resistant log of transactions, which in turn enables deterministic, self-enforcing actions based on predefined "if-then" logic (Racsko, 2019). This algorithmic rigidity, however, stands in stark opposition to the foundational commitments of a constitutional legal order. Public law is not a static, rigid system of absolute rules; it is intentionally designed to be contestable and adaptable. The law anticipates its own imperfection and therefore builds in mechanisms for *rectification and equitable discretion* (Davis, 1969). This flexibility is not a flaw in the legal system but rather one of its most critical features, allowing it to achieve substantive justice in a world of infinite complexity. As Aristotle noted, equity serves as "a correction of law where it is defective owing to its universality."

This capacity for correction is operationalized through several core legal principles. The most fundamental of these is *contestability*, the opportunity for individuals to dispute allegations or challenge the application of a rule, which has been described as the "very essence" of the rule of law (Yeung, 2017). A citizen has the right to challenge an administrative decision in court, and this right to a remedy is central to ensuring that state power remains accountable. Furthermore, public law empowers administrative officials with *discretion*, or a *margin of appreciation*, allowing them to make reasoned exceptions and temper the strict application of a rule to achieve a more proportional and equitable result in complex, multipolar relationships (Hermstrüwer, 2021).

Blockchain systems, by their very nature, struggle with these concepts. Designed to execute rules with deterministic finality, they are not built to recognize nuance, exercise compassion, or accommodate the inevitable ambiguities and instabilities that arise over time (Kohl, 2021). This turns their chief virtue, immutability, into what has been termed a "*vice of technocratic rigidity*" (Kohl, 2021). The irreversible nature of blockchain records is directly at odds with the need for contestation and the possibility of correcting initial errors, a conflict that becomes particularly acute when complying with rights-based challenges such as the right to rectification or erasure under the General Data Protection Regulation (GDPR) (Finck, 2018).

Smart contracts, being self-executing, can perfectly enforce obligations irrespective of whether the stipulated obligation is legally invalid or violates public law principles (Bell, 2021). This creates a perilous situation where the system can perversely lock both the administration and citizens into a state of illegality (Hermstrüwer, 2021). The integrity of the adjudication process and the ability to provide a legal remedy are profoundly undermined; while traditional courts can always order parties to perform an action or pay compensation, a court cannot typically compel a decentralized network to rewrite its executed code, making it technically impossible in some cases to restore violated legality (de Caria, 2021; G'sell & Martin-Bariteau, 2022). The "code" that enforces the rule thus lacks the interpretive flexibility and capacity for equitable judgment that is central to the "law," demanding that any digital governance system be designed not as an immutable fortress of logic but as a tool embedded within a broader institutional framework that preserves human oversight and meaningful contestation (Citron, 2007).

Another major tension arises from the conflict between emerging decentralized architectures and the hierarchical structures of legal accountability. Traditional public law is predicated on a clear chain of command and identifiable legal persons. If a government agency makes an unlawful decision, responsibility can be traced upwards through its organizational structure, and the courts know precisely whom to hold liable. Decentralized technologies, such as blockchain and especially more radical implementations like Decentralized Autonomous Organizations (DAOs), fundamentally disrupt this model (De Filippi & Wright, 2018). In a truly decentralized system, decisions may be executed automatically by smart contracts based on votes cast by a distributed and often pseudonymous network of participants. This presents a profound challenge to public law: if such a system violates a citizen's rights, who is legally responsible? The legal system is built to identify a legal person, an individual, a corporation, or a state agency, that can be sued, but a decentralized network, by design, often lacks any single point of control or identifiable legal entity (De Filippi et al., 2020).

This *distribution of agency* can all too easily become a *diffusion of responsibility*, creating a dangerous governance gap where rights can be violated without a clear path to a remedy (Werbach, 2018). In such a distributed system, it is exceptionally challenging to determine *who* is responsible for failures or illegal outcomes: is it the administrative agency that commissioned the system, the core developers who wrote the protocol, the nodes or miners who validate transactions, or some other intermediary? (De Gregorio, 2021; Reddick et al., 2021). This ambiguity makes it difficult for national laws to be enforced, as there is often no single, identifiable entity upon which government can exert pressure, unlike in traditional internet governance structures such as ICANN (De Filippi et al., 2020). The architectural choice to decentralize control thus predetermines a model of responsibility that is radically misaligned with the hierarchical expectations of public law, raising serious concerns for democratic values and creating the risk that the constitutional promise of accountability could be rendered obsolete by design (Finck, 2018).

3.3 Blockchain and New Public Governance

In response to these profound theoretical and practical challenges, the evolution of blockchain implementation in the public sector has increasingly aligned with the principles of *New Public Governance (NPG)*, a paradigm that reflects the realities of a digitally networked, interdependent, and pluralistic administrative landscape. This shift marks a crucial conceptual and operational transformation in how states envision technology's role in public administration, moving from hierarchical control and market efficiency toward *collaborative, trust-based governance* supported by technological infrastructures like blockchain.

3.3.1 From Bureaucracy to Networks: Setting the Context

To fully appreciate how blockchain resonates with the NPG model, it is first necessary to trace its departure from earlier paradigms of governance. *Weberian bureaucracy*, the classical model of public administration, was grounded in hierarchy, standardized procedures, and centralized

authority (Weber, 1922). It sought legitimacy through formal rationality, by ensuring that administrative decisions were predictable, rule-bound, and free from personal discretion. This model provided stability and legal certainty, particularly in states seeking to consolidate authority and enforce equality before the law. However, as governance tasks grew more complex and interdependent, the rigidity of bureaucratic control began to stifle responsiveness and innovation. Bureaucracy's strength, its procedural uniformity, became its main weakness when faced with dynamic, cross-sectoral problems that required flexibility and coordination across institutional boundaries.

In the late twentieth century, *New Public Management (NPM)* arose as a reformist response to these limitations (Hood, 1995). Influenced by neoliberal economics and private-sector practices, NPM introduced *market logics* into the public sector (Osborne, 2006). Efficiency, competition, and output measurement became the guiding principles of administrative reform (Rhodes, 1996). Governments began outsourcing functions to private contractors, restructuring agencies as quasi-autonomous entities, and adopting performance indicators to evaluate success. This managerial turn was designed to make governments "leaner and smarter." However, its emphasis on measurable performance and contractual accountability often fragmented public services. Inter-agency collaboration declined, and public administration risked being reduced to a set of transactions governed by contracts rather than relationships grounded in public trust. NPM achieved efficiency gains in some contexts, but it eroded the sense of shared mission and mutual dependence necessary for tackling collective challenges such as climate change, data governance, or public health crises.

3.3.2 The Emergence of New Public Governance

New Public Governance (NPG) emerged as a response to both the rigidity of Weberian bureaucracy and the instrumentalism of NPM. It reflects a more *networked, participatory, and inter-organizational* understanding of governance, acknowledging that the public sector operates within a pluralistic environment of stakeholders that includes private firms, civil society, academia, and citizens themselves (Brinkmann, 2021; Osborne, 2006). Rather than conceiving the state as a single hierarchical entity or a market regulator, NPG views governance as a process of *co-production*, a shared endeavor among diverse actors working toward collective outcomes (Rhodes, 1996).

At its core, NPG emphasizes *horizontal coordination* and *mutual interdependence*. Power is distributed across networks rather than concentrated in bureaucratic hierarchies. Decision-making occurs through negotiation, trust-building, and continuous dialogue rather than command and control. Accountability is reimagined as a *relational practice*, emerging from transparency, shared data infrastructures, and collaborative oversight. NPG's defining contribution lies in its reconceptualization of *public value*, not as something delivered by the state, but as something collectively created through partnerships and social innovation.

3.3.3 Blockchain and NPG: Conceptual Convergence

Blockchain technology fits naturally within this conceptual evolution. Its distributed ledger architecture, designed to record and verify transactions across multiple nodes without a central authority, mirrors the *decentralized, network-based* logic of NPG. In traditional bureaucratic systems, trust is guaranteed by hierarchical oversight and formal rules; in NPM systems, by competition and contractual enforcement. In contrast, blockchain builds trust through *transparency, verifiability, and immutability*, enabling multiple actors to cooperate without relying on a single intermediary (Pollicino & De Gregorio, 2021).

This alignment makes blockchain particularly well-suited for *multi-actor governance environments*, where various public and private institutions must collaborate while maintaining autonomy. For example, blockchain's *tamper-resistant records* can facilitate inter-agency data sharing without compromising confidentiality. Smart contracts can automate compliance across institutional boundaries, ensuring that agreed-upon actions occur transparently and predictably. These features embody NPG's ideal of "trust without hierarchy", a governance model sustained by openness and accountability rather than coercion or competition.

However, blockchain's contribution to NPG extends beyond operational efficiency. It redefines *institutional trust* itself. In traditional systems, trust resides in institutions and officials; in blockchain-enabled governance, it is partially relocated into code and cryptography. This shift creates both opportunities and tensions. While automation reduces the need for bureaucratic verification, it also risks displacing the *normative judgment and discretion* that democratic governance requires. NPG's framework helps balance this tension by insisting that technology remain embedded in human-centered networks of accountability, rather than replacing them.

3.4 Blockchain as an Enabler of Collaborative Public Value

Seen through the lens of NPG, blockchain provides a *technological substrate for co-production* in the public sector. It enables citizens, agencies, and private organizations to participate in shared decision-making processes while maintaining their individual sovereignty over data and operations. For instance, in public procurement or grant allocation, blockchain can ensure transparency and traceability, allowing multiple institutions to oversee disbursements simultaneously. In digital identity systems, it can support interoperable yet decentralized frameworks where citizens retain control over personal data, consistent with NPG's participatory ethos.

Yet, as NPG emphasizes, successful collaboration depends on more than technological interconnectivity, it requires *institutional capacity and governance design*. The distributed nature of blockchain challenges traditional lines of accountability: who is responsible when a smart contract fails or a consensus mechanism produces unjust outcomes? NPG provides a conceptual compass for addressing these questions. It suggests that responsibility in networked systems must be *shared and layered*, supported by transparent audit trails, participatory oversight, and adaptive regulation.

Moreover, blockchain can enhance NPG's vision of *public value co-creation* by enabling new forms of citizen participation. Token-based voting or participatory budgeting mechanisms, when designed ethically, can democratize governance processes. However, if implemented without safeguards, they risk reproducing inequalities through token concentration or technocratic exclusion. Thus, blockchain's integration into NPG demands *careful normative framing*, ensuring that technological inclusion translates into meaningful empowerment rather than mere procedural participation.

3.4.1 Institutional Adaptation and the Algorithmic State

As the *traditional administrative state* encounters the *algorithmic and distributed state*, NPG offers the theoretical scaffolding for integrating blockchain responsibly. It situates the technology within a broader continuum of democratic governance, recognizing that algorithms and ledgers are not substitutes for institutional judgment but instruments within a constitutional order. NPG's pluralist outlook acknowledges that governance is inherently political and interpretive: it requires balancing efficiency with fairness, and transparency with privacy.

In this respect, the intersection of blockchain and NPG illuminates a central insight: *decentralization is not an end in itself*, but a design principle to be operationalized within democratic institutions. Blockchain can strengthen transparency and trust, but only if it is governed by frameworks that preserve human accountability, procedural justice, and ethical oversight.

3.4.2 From Theory to Translation

This conceptual bridge leads directly to the next stage of analysis, the *translation of blockchain's ideological and technical attributes into practical tools of governance*. The tension between the deterministic logic of blockchain and the discretionary nature of administrative law compels governments to reinterpret decentralization, transparency, and immutability within constitutional and regulatory contexts. This act of translation is inherently *political and normative*, involving choices about what aspects of blockchain to adopt, constrain, or repurpose. The resulting design decisions will determine whether blockchain becomes a tool for democratic empowerment or a mechanism of technocratic control.

In sum, the convergence of blockchain and New Public Governance represents both a theoretical synthesis and a practical challenge. It reveals how governance in the digital age must evolve, not by abandoning law and institutions, but by *reimagining them as components of a networked, co-productive ecosystem*. Blockchain's promise lies not merely in decentralizing data, but in decentralizing trust itself, an ambition that only the principles of NPG can ground in legitimacy, accountability, and collective purpose.

The preceding discussion of *blockchain and New Public Governance (NPG)* establishes the conceptual foundations for understanding how decentralized technologies align with the evolving paradigms of public administration. It demonstrated that blockchain's distributed architecture resonates with NPG's emphasis on horizontal coordination, inter-organizational trust, and co-production of public value. However, while this theoretical alignment provides a compelling vision of participatory and transparent governance, the actual implementation of blockchain within governmental systems requires a more granular examination of its *technical affordances and design constraints*. The ideals of NPG must ultimately be translated into the operational language of algorithms, ledgers, and protocols, each of which embodies specific assumptions about authority, accountability, and control.

Thus, the next section moves from the *normative and institutional dimension to the technical and architectural level* of blockchain's integration into public governance. It investigates how the core properties of the technology, decentralization, immutability, transparency, and automation, are reinterpreted when placed within administrative and legal contexts. This transition is critical because it marks the point where philosophical aspirations encounter the practical realities of bureaucratic operation, data protection law, and institutional legitimacy.

3.5 The Technical Properties of Blockchain in the Governmental Design

The profound tensions between the deterministic logic of blockchain and the discretionary nature of constitutional law have forced a pragmatic evolution in how the technology is implemented within the public sector as explained in the previous sections. The journey from abstract, anti-statist rhetoric to concrete administrative application requires a crucial process of translation, where the intrinsic technical properties of blockchain are reinterpreted and adapted to serve governmental objectives. This process of translation is not neutral; it is an inherently political act of design that determines which features of the technology are maximized, which are suppressed, and how foundational public values like legality, accountability, and privacy can be reconciled with the capabilities of a distributed ledger. The resulting design choices reveal a consistent pattern of co-option, where the radical decentralizing potential of the technology is tamed in favor of creating more resilient and efficient systems of inter-organizational coordination under the firm oversight of state authority.

This translation is evident in the reinterpretation of blockchain's core properties. In its original conception, *decentralization* was positioned as a tool to eliminate central institutional control. In the governmental context, however, its function is more accurately described as *distributed administration* (Bustamante et al., 2022). Rather than dissolving centers of power, this approach shifts the focus from a single point of failure (SPOF) to a more resilient system where multiple, often sovereign, governmental or private entities can jointly manage a shared ledger while simultaneously maintaining sovereign control over their own internal data and repositories (Bustamante et al., 2022; Fridgen et al., 2019). This allows for enhanced coordination among different government bodies without requiring them to delegate governance to a single, overarching central authority. Analysts rightly caution, however, that the mere distribution of data

across many nodes does not automatically equate to the decentralization of power, which must be assessed by examining the governance model of the entire ecosystem (Clifton & Pal, 2022).

Similarly, the property of immutability, is repurposed for administrative ends. For the state, this characteristic is highly valuable for enhancing *auditability* and ensuring the integrity and irrevocability of public records, such as property titles, academic credentials, or archival documents (Bustamante et al., 2022; Sobolewski & Allesie, 2021). Yet this same property represents one of the technology's most significant limitations for public administration, as its rigidity applies equally to correct and erroneous data. The old computing adage "garbage in, garbage out" takes on a new and perilous meaning when the "garbage" is permanently and irrevocably inscribed on a distributed ledger, posing a profound legal challenge to the principles of correction and contestability (Alston, 2019; Berryhill et al., 2018).

The property of *transparency* is also adapted; while public blockchains can provide what some have called "perfect transparency," allowing any interested party to read the entire ledger (G'sell & Martin-Bariteau, 2022), in a public setting this is leveraged more selectively to generate trust and accountability for specific processes, with verifiability allowing participants to independently check the correctness of the system's state using cryptographic proofs (Caradonna, 2020). When applied thoughtfully, this selective transparency can *empower citizens by reducing opportunities for corruption and fraud*, fostering greater confidence in public administration. However, it also brings privacy and data protection risks.

Perhaps the most critical stage of translation lies in the automation of administrative functions through smart contracts. These deterministic, rule-based algorithms are praised for their capacity to streamline bureaucratic processes by automatically enforcing obligations such as distributing social benefits, processing payments, or issuing licenses (Boeding, 2024; Goossens, 2021). Automation promises increased efficiency, transparency, and consistency while minimizing administrative costs and human error. Yet, this technological precision also introduces rigidity. Smart contracts lack the flexibility to account for context, equity, or proportionality, principles central to the rule of law (Alston, 2019). Accordingly, their implementation must be carefully limited to processes requiring no interpretive or discretionary judgment.

The most critical design decision in this entire translation process, the one that defines the governance architecture and dictates how these properties are balanced, is the choice of the blockchain type. The public sector has shown a clear and overwhelming preference for *permissioned (private or hybrid) systems*¹, largely avoiding the public permissionless model of cryptocurrencies like Bitcoin (Atzori, 2017). This choice is driven by the inherent drawbacks of permissionless systems for public service delivery, including poor scalability, high energy and transaction costs (often involving cryptocurrency tokens for incentives), a lack of transaction

¹ *Permissionless blockchains* (such as Bitcoin or Ethereum) are open networks where anyone can participate in validating transactions and maintaining the ledger without prior authorization. They rely on public consensus mechanisms (e.g., Proof of Work or Proof of Stake) and typically feature full transparency and pseudonymity. In contrast, *permissioned blockchains* restrict participation to vetted entities, such as government agencies or authorized private partners, operating under predefined governance rules. These systems prioritize scalability, privacy, and regulatory compliance over absolute openness, making them more suitable for institutional and public-sector applications.

secrecy, and intractable governance difficulties stemming from their pseudo-anonymity (Reddick et al., 2021; E. Tan et al., 2022). Permissioned architectures, by contrast, allow public authorities to create a controlled and legally compliant environment. They offer clearer governance, as rules and access rights can be designed and coordinated with known and vetted participants, enabling necessary human intervention and oversight (Guegan, 2017). They also deliver the high throughput and low latency required for mass-scale public services and, most importantly, provide the control necessary to manage identities and comply with stringent legal frameworks, especially data protection regulations like the GDPR (Batubara et al., 2018; Reddick et al., 2021).

This deliberate architectural choice effectively redefines what "decentralization" means in the public sector. Instead of a radical, trustless network of anonymous peers, it becomes a system of *federated data governance* within a controlled and legally accountable framework. This model allows the state to retain the key architectural benefits of a distributed ledger, a shared, tamper-resistant record and enhanced resilience, while ensuring that the system remains under the purview of public law. The government's role in this configuration shifts from being the sole intermediary to acting as a *trusted platform provider or steward*, who initiates the network, defines the rules of engagement, and audits applications to ensure their proper functioning and accountability (Ølnes et al., 2017).

Despite the careful design choices intended to mitigate risk, the path to widespread adoption is impeded by a series of decisive bottlenecks that are primarily non-technical in nature. Systematic reviews of blockchain trials repeatedly confirm that the greatest obstacles are not the cryptographic primitives or the software itself, but rather systemic challenges related to *governance, legal clarity, and organizational readiness* (Bosch et al., 2022; Cagigas et al., 2021; E. Tan et al., 2022). Regulatory uncertainty is consistently identified as the most significant risk associated with blockchain adoption for governments (Cagigas et al., 2021). A lack of a mature legal framework frequently prevents successful pilots from transitioning into daily operational use (Bosch et al., 2022). Key legal issues include the uncertain status and recognition of data notarized on a blockchain and the questionable validity of digital signatures for critical public functions like property transfers, often necessitating continued reliance on traditional paper-based processes. Furthermore, the transnational nature of many potential applications requires international policy coordination to establish common data standards and resolve jurisdictional conflicts, a collective action problem that remains largely unsolved (Bank of Canada & Monetary Authority of Singapore, 2019; Cagigas et al., 2021).

Alongside legal ambiguity, the introduction of blockchain demands fundamental changes in organizational responsibilities and governance approaches that public administrations are often ill-equipped to handle (Ølnes et al., 2017). The performance of any blockchain network depends not only on its internal coded rules but also on the proper functioning of *external institutional frameworks* (Alston, 2019; Bustamante et al., 2022). The benefits of the technology are therefore often contingent upon large-scale institutional adjustment and reorganization, not mere technological installation (Brinkmann, 2021). Public administrations, however, frequently suffer from deep-seated *organizational inertia* and may lack the internal capacity, skills, and agile mindset needed to design, maintain, and govern complex blockchain applications (Business & Information Systems Engineering of the Fraunhofer FIT & Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, 2022). As former government officials

have acknowledged, the public sector struggles to compete with the private sector for the necessary data science and engineering talent, making it difficult to build and retain the required capacity (Ølnes et al., 2017; Swan, 2015).

3.5.1 Data Protection as a Hard Constraint on Blockchain

Among the array of non-technical bottlenecks impeding the adoption of blockchain in the public sector, an important one is the legal framework for data protection, particularly the European Union's General Data Protection Regulation (GDPR). The regulation, designed primarily with centralized databases and clear institutional actors in mind, creates a fundamental and unavoidable tension with the decentralized, immutable, and often pseudonymous nature of distributed ledger technology (Finck, 2018). This collision of paradigms is not a minor hurdle to be overcome with a simple technical fix; it represents a hard constraint that forces a radical rethinking of how blockchain can be responsibly deployed by the state. The legal obligations enshrined in the GDPR have become a primary driver compelling public administrations to abandon the ideological purity of permissionless systems in favor of controlled, hybrid architectures that subordinate technological capabilities to legal necessity.

The most direct and irreconcilable conflict arises between blockchain's core feature of immutability and the fundamental rights granted to data subjects under the GDPR. At the heart of the regulation are Article 16, the *right to rectification*, which allows individuals to correct inaccurate personal data, and Article 17, the *right to erasure*, more famously known as the "right to be forgotten". These rights are essential safeguards, ensuring that individuals retain a degree of control over their personal information and are not perpetually haunted by data that is incorrect, irrelevant, or unlawfully processed. The very design of blockchain, however, is intended to prevent the alteration or deletion of records once they have been validated and added to the chain. This permanence, while beneficial for auditability, becomes a critical liability when personal data is involved. If incorrect personal information is permanently recorded on a public ledger, remediation becomes not just legally challenging but often technically impossible. This rigidity can lock both the administration and citizens into a state of perpetual illegality, where a simple error cannot be corrected, and a lawful request for deletion cannot be honored (Fridgen et al., 2019). Furthermore, the permanence of data on an append-only ledger is fundamentally at odds with core GDPR principles like *purpose limitation and data minimization*, which mandate that personal data should not be kept longer than is necessary for the specific purpose for which it was collected (Goossens, 2021).

This foundational conflict is compounded by a second, equally significant challenge to the GDPR's accountability framework: the difficulty of identifying the *Data Controller*. The GDPR's entire enforcement model rests on the ability to designate a specific legal person, the controller, who determines the purposes and means of data processing and is therefore legally responsible for compliance (Goossens, 2021; Reddick et al., 2021). In a traditional, centralized system, this role is easy to assign. In a public, permissionless blockchain, however, where every node in the network processes and holds a copy of the same data, identifying a singular or even a group of joint controllers becomes an exercise in legal futility (Pollicino & De Gregorio, 2021). This ambiguity

creates a vacuum of responsibility, leaving individuals with theoretical rights but no clear entity to hold accountable for respecting them (De Filippi et al., 2020).

It is this critical need for identifiable accountability that has decisively pushed governmental implementations toward *private or consortium blockchains*. In these permissioned systems, where participation is restricted to known and vetted entities, the controller (or joint controllers) can be clearly and easily identified (Reddick et al., 2021). This allows the public agency or the consortium of participating bodies to be explicitly designated as the legally responsible party, thereby satisfying the GDPR's structural requirements (De Hert & Kumar, 2021). In cases involving multiple agencies, this often necessitates the drafting of formal *joint control arrangements* through administrative agreements that precisely delineate the respective responsibilities for compliance and establish the lawful bases for data processing (Fridgen et al., 2019). This deliberate architectural choice is a direct concession to legal reality, demonstrating how constitutional and statutory requirements actively shape the technological form.

To mediate these deep-seated tensions, system designers have developed a set of architectural workarounds and compliance patterns. The most prevalent of these is the use of a *hybrid, GDPR-compliant architecture* that separates personal data from the immutable ledger. In this model, sensitive personal data is stored *off-chain* in a conventional, centralized database where it can be managed, corrected, and deleted in compliance with the law. The blockchain itself is then used to store only cryptographic references or hashes pointing to that off-chain data (Berryhill et al., 2018; Reddick et al., 2021). This approach seeks to capture the best of both worlds: the integrity, auditability, and tamper-resistance of the blockchain for process verification, and the flexibility and legal compliance of traditional databases for data storage (Fridgen et al., 2019).

This is often combined with strong *pseudonymization techniques* applied to any data that must reside on the chain. This requires the creation of highly secure *off-chain attribution mechanisms* that can, when legally required and authorized, link the pseudonymous on-chain data back to a natural person (Fridgen et al., 2019; Goossens, 2021). Advanced cryptographic methods, such as *zero-knowledge proofs*², are also being explored to allow for the verification of a piece of information (e.g., "this person is over 18") without revealing the underlying personal data itself (e.g., their date of birth), thereby adhering to the principles of data minimization and privacy by design (Goossens, 2021). These technical solutions, however, are not panaceas. They must be embedded within a rigorous governance process that begins long before the first line of code is written. Legal safeguards must be addressed *ex ante* through the principle of *Data Protection by Design*, which obligates organizations to conduct a formal *Data Protection Impact Assessment (DPIA)* for any project likely to result in a high risk to individuals' rights and freedoms (Finck, 2018; Goossens, 2021). This assessment forces administrations to analyze the necessity of using blockchain, weigh the risks posed by perpetual storage and decentralization, and ensure that the

² *Zero-knowledge proofs (ZKPs)* are cryptographic protocols that allow one party (the prover) to demonstrate to another (the verifier) that a specific statement is true without revealing any underlying information beyond that fact. In other words, they enable verification of data or transactions without disclosing the data itself. In blockchain systems, ZKPs enhance privacy and security by allowing validation of transactions, credentials, or computations while keeping sensitive details, such as identities or amounts, completely confidential (Zein & Pinkwart, 2025).

chosen architecture adheres to all processing principles from the very outset (De Hert & Kumar, 2021).

A compelling real-world example of these compliance patterns in action is the pilot project conducted by *Germany's Federal Office for Migration and Refugees (BAMF)* to coordinate the national asylum procedure (Fridgen et al., 2019). The project faced the immense challenge of improving communication and workflow management among numerous federal and state authorities, each with its own separate competencies and data systems (Business & Information Systems Engineering of the Fraunhofer FIT & Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg, 2022). The solution was a carefully designed, GDPR-compliant blockchain system built on a *private, permissioned architecture* that used private data collections to strictly limit access to sensitive information. The system successfully demonstrated how a *pseudonymization approach combined with a highly secure off-chain attribution mechanism* could enable the efficient and secure exchange of process-relevant information, thereby addressing the challenges of Germany's decentralized federal structure while fully respecting the stringent requirements of European data protection law (Fridgen et al., 2019). This case stands as a crucial proof of concept, illustrating that while the collision between blockchain and the GDPR is severe, it can be navigated through meticulous, legally-informed design.

3.6 Public Sector Applications: From Pilot to Practice

The theoretical tensions and practical design constraints discussed previously are not merely abstract concerns; they are actively shaping a diverse and growing landscape of real-world blockchain initiatives across the public sector. An examination of these applications, which range from conceptual proposals and early-stage pilots to a handful of fully implemented systems, provides invaluable insight into how governments are navigating the governance paradox by translating technological potential into administrative reality (Alessie et al., 2019; Berryhill et al., 2018). These initiatives consistently seek to leverage blockchain's core features, such as immutability, transparency, and decentralized transaction handling, to achieve long-standing administrative goals, including increasing efficiency, reducing bureaucracy, and enhancing public trust (Alessie et al., 2019). A systematic review of these use cases, categorized by their core governmental function, reveals distinct patterns of adoption, demonstrating a clear preference for pragmatic, incremental improvements over radical, disruptive transformation.

One of the most promising and actively explored areas for public sector blockchain application is *Identity Management and Verifiable Credentials*. This domain is a primary focus because a secure and reliable identity is the cornerstone of the modern state-citizen relationship and a prerequisite for virtually all digital public services. The technology offers a pathway toward a model of *Self-Sovereign Identity (SSI)*, which promises to give individuals greater control and ownership over their personal data by allowing them to manage their own credentials in a secure digital wallet (Bosch et al., 2022). Yet, in a clear illustration of the governance paradox, most practical implementations reveal that the foundational authentication of the personal information stored in these decentralized services still requires a government or other trusted party to issue and

attest to the credentials in the first place (Bustamante et al., 2022). The state, far from being disintermediated, retains its crucial role as the root authority for identity verification.

Estonia stands as a prominent pioneer in this domain, with one of the world's most technologically advanced national ID-card systems that is mandatory and grants citizens access to a wide array of secure e-services, including e-voting, national health insurance, and medical records administration (A. J. Zwitter et al., 2020). Its system uses Keyless Signature Infrastructure (KSI) technology, which the Estonian government refers to as blockchain, to ensure the integrity of its digital public services through hash-based verification (Cagigas et al., 2021; A. J. Zwitter et al., 2020). Another significant application is the management of academic credentials, a field ripe for innovation due to issues of fraud and cumbersome verification processes. The nation of **Malta**, for example, launched an initiative in October 2017 to use the open-source Blockcerts standard for managing academic records (Alessie et al., 2019). This made Malta the first country to nationally introduce blockchain-driven diplomas, an implementation targeted specifically at improving certification and validation processes and ensuring credentials are both tamper-proof and easily verifiable by employers or other institutions (Alessie et al., 2019; Bosch et al., 2022; Komorowski et al., 2022). Similar state-funded initiatives for digital diplomas are underway in jurisdictions like *Luxembourg* and *India*, all aiming to leverage blockchain's permanence and security for academic credentials (Komorowski et al., 2022). On a more local level, the city of *Zug, Switzerland*, allows its citizens to register for a blockchain-based identity (eID) that can be used for authentication for municipal services like electronic voting (Brinkmann, 2021; Reddick et al., 2021). These initiatives are complemented by broader international efforts like the *ID2020 Alliance*, a public-private partnership focused on creating universal, blockchain-enabled identity solutions, particularly for vulnerable populations without official documentation (Berryhill et al., 2018; A. J. Zwitter et al., 2020).

A second major category of application is the management of *Public Records and Registries*. This area is a natural fit for blockchain, as its core value proposition of creating an immutable, transparent, and auditable ledger directly addresses the foundational requirements of public record-keeping. Perhaps the most highly publicized success story is the *Land Title Registry in the Republic of Georgia*. In a partnership with the private sector, the government used blockchain to secure and streamline the process of recording land titles, with dramatic results: the registration of extracts became 400 times faster, and associated costs were reduced by over 90% (Bustamante et al., 2022; Cagigas et al., 2021). The technology's potential to enhance transparency and reduce vulnerability to corruption or fraudulent land expropriation is especially valuable in contexts where public trust in governmental institutions is low, providing a cryptographically secure foundation for property rights (Bustamante et al., 2022; Cagigas et al., 2021). Following this model, *Sweden* has also pursued the Exonum project focused on the registration, verification, and transfer of land titles (Reddick et al., 2021). In the United States, the state of *Delaware's* Public Archives partnered with a distributed ledger startup to archive state records on a blockchain, aiming to better secure government records and reduce opportunities for fraud (Bustamante et al., 2022). The technology is also being applied to health records; *Estonia* uses a hash-based integrity check for its national electronic health records system (e-Estonia, n.d.), while the *U.S. Food and Drug Administration's* Oncology Center of Excellence has operated a blockchain-based platform for information exchange (Dimitrov, 2019).

The realm of *Financial Management and Social Transfers* represents a third critical area of application, where smart contracts and digital currencies are used to automate transactions, redistribute public funds, and enhance efficiency and oversight. A leading operational example is the "*Stadjerspás*" smart voucher system in Groningen, Netherlands. A fully operable service since 2016, it uses a blockchain infrastructure to distribute discounted services to low-income citizens. By utilizing programmable money flows and smart contracts, the system can enforce detailed spending conditions, ensuring that public money is spent exclusively for its specified purpose and is targeted only to the intended beneficiaries, representing a significant innovation in policy compliance (Komorowski et al., 2022). Central banks are also actively exploring the technology; the Monetary Authority of Singapore led *Project Ubin*, a multi-phase project investigating the use of blockchain for government securities transactions and inter-bank payments (Berryhill et al., 2018). The system was designed to operate 24/7 with minimal human intervention, reducing the complexity of balancing accounts (Bustamante et al., 2022). This is part of a broader global trend of Central Bank Digital Currency (CBDC) initiatives, with countries like Canada (through its CAD-COIN experiment) also experimenting with their own digital currencies built on blockchain platforms (Berryhill et al., 2018; Bosch et al., 2022). Conceptual applications have also been proposed for improving the transparency and efficiency of federal grant management in the *United States*, aiming to reduce redundant reporting burdens for recipients (Komorowski et al., 2022).

Finally, blockchain is being explored by international organisations and scholars for its potential to transform *Governance and Democratic Processes*, enhancing transparency and creating new forms of citizen participation (World Economic Forum, 2020). Public procurement is a key target for reform, as it is an area often vulnerable to corruption. *Ukraine*, for instance, has implemented or explored a decentralized blockchain e-auction system as part of its public procurement management, a move intended to increase transparency and support disintermediation (Bosch et al., 2022; Komorowski et al., 2022). Similarly, a prototype developed during a hackathon in *Mexico* uses smart contracts to make the public bidding process for tenders more reliable, transparent, and open to citizen participation, aiming to ensure the winner generates greater social benefit (Berryhill et al., 2018; Komorowski et al., 2022). Electronic voting remains a widely discussed, if controversial, application, with various states and international bodies, including *Switzerland* and the *EU*, testing potential solutions to improve the efficiency and reliability of voting procedures and their monitoring (G'sell & Martin-Bariteau, 2022). At the far end of the ideological spectrum lie projects like *Bitnation*, developed by evangelists of decentralization to create *cryptonations*, stateless, do-it-yourself governance services running entirely on the blockchain, representing the purest form of the techno-libertarian vision that stands in stark contrast to these pragmatic, state-led adoption efforts (Atzori, 2017).

3.6.1 Synthesizing the Evidence: Patterns and Paradoxes in Public Sector Adoption

The diverse typology of applications, from land registries in the Caucasus to social welfare programs in the Netherlands, provides a rich empirical basis from which to draw broader conclusions about the state of blockchain adoption in the public sector. When analyzed collectively, these case studies reveal several consistent patterns and recurring paradoxes that

define the technology's current trajectory. Far from ushering in a revolutionary era of stateless governance, the evidence points toward a much more pragmatic and incremental process of integration. This process is characterized by a clear set of governmental priorities, a distinct architectural preference driven by legal and operational realities, and a persistent set of challenges that continue to impede the transition from promising pilots to large-scale, transformative policy.

A primary insight gleaned from this evidence is the overwhelming focus on achieving *incremental efficiency gains rather than radical transformation*. While blockchain was once heralded as a disruptive force, the majority of ongoing projects, particularly in Europe, are concentrated on automating the enforcement of transactions, reducing bureaucracy, and cutting administrative costs in areas like record-keeping and financial management (Alessie et al., 2019). These efforts represent valuable, but ultimately incremental, improvements to existing processes, not the fundamental shifts in governance that early proponents envisioned. This pattern strongly supports the thesis that the public sector is engaged in a period of cautious institutionalism, seeking to harness the technology as a tool for administrative optimization rather than as an instrument of political revolution.

A second, and perhaps the most telling, pattern is the *overwhelming preference for permissioned systems*. Across the wide range of operational projects, virtually none utilize a purely public, permissionless archetype (Reddick et al., 2021). Instead, public administrations consistently opt for *private permissioned blockchains* or hybrid models, where the right to read the ledger and, more importantly, to validate transactions is restricted to a pre-approved set of known nodes, often comprised of governmental agencies and trusted consortium members (Reddick et al., 2021). This critical design choice is not arbitrary; it is a direct and necessary response to the stringent requirements of public administration. The need for legal compliance (such as with data protection regimes like the GDPR), the demand for governmental oversight, and the necessity of maintaining control over the ledger for high-volume transactions, such as those in pension systems or property transfers, make the open and anonymous nature of permissionless chains untenable for most state functions (Reddick et al., 2021).

Third, the case studies demonstrate that the potential benefits of blockchain, particularly its ability to ensure data integrity, enhance transparency, and mitigate fraud, tend to be most significant in *low-trust environments*. The technology is frequently cited as especially advantageous for *developing countries or jurisdictions characterized by high levels of corruption or weak public confidence in state institutions* (Cagigas et al., 2021). The well-known example of the *land registry project in the Republic of Georgia* illustrates this potential vividly: by employing a cryptographically secure and transparent ledger, the system established a verifiable foundation for property rights and market confidence in a context where institutional trust was historically fragile (Cagigas et al., 2021). However, the mere adoption of blockchain does not, by itself, generate trust where it is otherwise absent. The *Russian blockchain voting initiative* provides a cautionary example: although the system was publicly presented as an effort to improve electoral transparency and efficiency, the process remained opaque and shielded from independent scrutiny (Vakarjuk et al., 2022). The state retained full control over the infrastructure, and no verifiable documentation of the voting process was made available. Consequently, many citizens perceived the results as manipulated, reinforcing rather than resolving the underlying trust deficit. This example underscores that, while blockchain is often expected to yield the greatest benefits in low-trust

settings, such environments also pose the highest risks for its misuse. Without adequate institutional safeguards, the technology can become a tool of control rather than an instrument of accountability. To ensure that blockchain functions as a genuine solution rather than an enabler of corruption and fraud, a baseline level of institutional and procedural trust must be established. This can be achieved through independent audits, external observation, and transparent implementation processes, which collectively ensure that technological assurances of integrity are matched by genuine accountability in practice.

Despite the institutional focus, many pilot projects exhibit a strong orientation *toward citizen-centric services*. A significant number of initiatives are focused on enhancing citizen self-sovereignty and improving the user experience of interacting with the state. This is most evident in digital identity management projects, such as the eID in Zug, Switzerland, which aim to give citizens greater control over their personal data (Alessie et al., 2019; Reddick et al., 2021). Mobile applications, like the one used for the Stadterspas program in Groningen, allow citizens to interface remotely with public administration, eliminating the need for hard copies and in-person visits to government offices (Alessie et al., 2019). Finally, the evidence underscores the persistent *challenges to scaling and achieving legal certainty*. Although many proof-of-concept projects are deemed successful on a technical level, very few have been scaled up to become national policy, indicating significant hurdles to widespread adoption (Bustamante et al., 2022). A primary obstacle is the lack of a clear and mature legal framework, which often prevents successful pilots from moving into daily operations. For example, the uncertain legal recognition of data notarized on a blockchain or the validity of digital signatures for critical public transactions frequently means that new digital processes cannot fully replace their legally mandated paper-based counterparts (Bosch et al., 2022). To illustrate this dynamic in practice, the city of Zug's blockchain-based digital identity pilot allowed residents to access various municipal services and even participate in local decision-making processes. The project was technically successful, demonstrating the feasibility of using decentralized identity solutions for public administration (Bitcoin Magazine, 2018). However, despite its promising start, the initiative has remained in a pilot phase for over four years and has not yet been integrated into the city's permanent digital infrastructure. The principal barrier to its broader implementation has been citizen concerns regarding data protection and privacy (Geiser, 2021). Many residents expressed uncertainty about how their personal data might be processed, stored, or shared within the blockchain ecosystem, raising questions about whether existing legal frameworks are adequately equipped to safeguard individuals' rights. This case highlights that even in technologically advanced and high-trust jurisdictions, public confidence in legal protections remains a decisive factor for the large-scale deployment of blockchain-based identity systems.

These observed patterns are rooted in the tangible benefits that blockchain can offer when its properties are correctly aligned with the functions of public administration. The technology's value proposition centers on its inherent capacity to improve data management and create more resilient oversight mechanisms. The core characteristics of irreversibility, transparency, and auditability are highly attractive for governmental functions that depend on the integrity of their records (Atzori, 2017). Compared to traditional centralized master-slave databases, permissioned blockchain architectures provide significant advantages in *data integrity, availability, and error reduction* (Komorowski et al., 2022). The distributed and cryptographically-linked nature of the ledger ensures that data, once recorded, is exceedingly difficult to manipulate without leaving a

trace, creating a system where the stored information corresponds closely to reality (Ølnes et al., 2017). This capability allows for the establishment of a "*single source of truth*" that can be shared across multiple, often siloed, organizations, thereby eliminating the endless necessity of copying and reconciling the same data between disparate IT systems (Ølnes et al., 2017).

From this foundation of data integrity flow the primary benefits of *efficiency and enhanced oversight*, which governments consistently prioritize (Cagigas et al., 2021). Efficiency gains are realized most directly through the automation of transactions and workflows via smart contracts, which can significantly *reduce bureaucracy, administrative costs, and the potential for human error* (Reddick et al., 2021). Automating processes for eligibility verification or the disbursement of payments, for instance, can reduce transaction costs for both the government and its citizens, streamlining procedures like tax refunds or grant management (Boeding, 2024). Simultaneously, the append-only nature of the ledger enhances oversight by ensuring the *irrevocability of records* and dramatically increasing the auditability of data (Sobolewski & Allessie, 2021). This improved transparency is a critical component for bolstering public integrity, as it can enable regulators to monitor a system without information asymmetry and to *immediately detect hazards or irregularities* in a way that is not possible with opaque, centralized databases (Reddick et al., 2021).

3.7 Decisive Bottlenecks and Systemic Risks in Public Administration

While the potential benefits of blockchain in enhancing data integrity and administrative efficiency are compelling, a clear-eyed assessment of the technology's integration into the public sector reveals a formidable array of challenges and risks. These obstacles, rooted primarily in non-technical domains, act as decisive bottlenecks that impede widespread productionization and temper the more utopian expectations associated with the technology (Ølnes et al., 2017). Systematic reviews of various trials repeatedly confirm that the most critical barriers are not the intrinsic technical challenges of cryptography, but rather the profound difficulties related to *governance, legal clarity, and organizational readiness* (Tan et al., 2022). These systemic issues, combined with persistent technical constraints and significant equity concerns, demand careful consideration and strategic mitigation by any public administration seeking to responsibly adopt distributed ledger technologies.

The most significant and consistently identified risk is the pervasive *regulatory uncertainty and lack of a mature legal framework* (Cagigas et al., 2021). This legal ambiguity often creates a chilling effect, preventing successful pilot projects from transitioning into fully operational, daily use systems (Bosch et al., 2022). A primary issue is the uncertain *legal recognition of data* itself. For many key public functions, such as property transfers or the issuance of official certificates, the legal validity of data notarized on a blockchain or of digital signatures executed via smart contracts is either unclear or impermissible under current law. This forces a continued and often inefficient reliance on traditional, paper-based documents, undermining the potential benefits of a fully digital process. This problem is compounded at the international level by the urgent need for *policy coordination*, especially for applications involving cross-border supply chains and

payment systems (Bank of International Settlements Basel Committee, 2021; Cagigas et al., 2021). The absence of common data standards and harmonized regulatory requirements across different jurisdictions creates significant collective action problems, resulting in a fragmented technological landscape that inhibits interoperability (Bank of Canada & Monetary Authority of Singapore, 2019).

Intricately linked to these legal hurdles are the deep-seated *governance challenges and the question of organizational readiness*. The shift from centralized databases to distributed ledgers is not a simple technological upgrade; it necessitates fundamental changes in institutional responsibilities and requires the development of entirely new governance approaches (Ølnes et al., 2017). The performance and legitimacy of any blockchain network depend not only on the proper functioning of its internal, code-based rules but also, and more importantly, on the robustness of *external institutional frameworks* that provide oversight and accountability (Alston, 2022; Bustamante et al., 2022). Consequently, the benefits of blockchain are often contingent upon large-scale *institutional reorganization and adjustment*, a far more complex undertaking than mere technological installation (Brinkmann, 2021). Public administrations, however, are frequently characterized by significant *organizational inertia* and often lack the internal capacity, specialized skills, and agile culture needed to design, maintain, and govern complex blockchain applications. As many government officials have acknowledged, public sector salaries and procurement processes make it exceedingly difficult to hire and retain the necessary data scientists and cryptographic experts, who are in high demand in the private sector (Ølnes et al., 2017; World Economic Forum, 2020).

This dynamic gives rise to another paradoxical risk: the *threat of new forms of centralization and vendor lock-in*. As previously discussed, the practical need for control, performance, and legal compliance has led governments to overwhelmingly favor *private permissioned blockchains* or hybrid models (Atzori, 2017; Sobolewski & Allestie, 2021). While this choice is necessary, it risks creating new monopolies, where a few large private companies or powerful consortia with the requisite technical capacity gain considerable and potentially unaccountable power over critical public sector infrastructure (Reddick et al., 2021). In these scenarios, governance does not emerge spontaneously as a decentralized public good; it must be deliberately established and is often dictated by a small group of technical experts or corporations (Berryhill et al., 2018). To mitigate this risk, many see the promotion of *open-source standards and documentation* as a critical strategy. Openness can enhance the effectiveness of the technology, speed up development, and, most importantly, facilitate the interoperability needed to prevent the public sector from being locked into a single proprietary vendor or technology (Reddick et al., 2021).

Alongside these overarching governance issues, several *technical and operational constraints* remain significant barriers to adoption. *Scalability* continues to be a primary technical limitation, particularly for large-scale applications that must manage a high volume of transactions, such as national pension systems or VAT collection (Reddick et al., 2021). Distributed solutions are fundamentally *less efficient* and more difficult to scale up to higher capacity than their traditional centralized database counterparts (Atzori, 2017; Bustamante et al., 2022). Furthermore, in a distributed architecture, modifying a protocol or fixing a bug requires achieving a wide consensus among developers and nodes, a process that can be far more complex and time-

consuming than updating a centralized system, thereby inhibiting a timely response to unexpected challenges (Ølnes et al., 2017).

The lack of standardized protocols also creates severe *interoperability impediments*, resulting in a fragmented technological landscape that hinders the deployment and scaling of blockchain solutions (Sobolewski & Allessie, 2021). The low percentage of identified *cross-border* cases in Europe highlights the currently low level of interoperable services between nations (Bosch et al., 2022). For blockchain technology to evolve from a collection of isolated, idiosyncratic platforms into a comprehensive information infrastructure, the establishment of common standards and interoperability structures is essential (Sobolewski & Allessie, 2021). Pan-national initiatives like the European Blockchain Service Infrastructure (EBSI) are attempting to address this very problem by providing a standardized infrastructure designed to overcome these cross-border challenges, particularly for verifiable credentials (E. Tan et al., 2022). Finally, the *sustainability and cost profiles* of blockchain must be carefully assessed. While cost reduction is a major driver of adoption, the high energy consumption requirements of legacy proof-of-work protocols are difficult to justify for public initiatives, necessitating the options of less computationally demanding consensus algorithms (Cagigas et al., 2021; Ølnes et al., 2017). Moreover, although operational costs can be dramatically reduced, as seen in the Georgia land title registry case, the initial *transition costs* required to switch from existing legacy systems to new blockchain solutions can be substantial for government agencies (Cagigas et al., 2021).

Finally, the most significant risk at stake is a profound paradox: if not thoroughly evaluated and carefully governed, the very features of blockchain designed to empower citizens against central intermediaries, such as immutability and transparency, can be repurposed *by* those intermediaries as powerful new tools of surveillance and control. Mitigating this and other threats requires more than technical proficiency; it demands a deep understanding of the technology's limitations and a firm grounding in public needs and values. Ultimately, a successful application in this sensitive domain hinges on achieving this difficult balance.

3.7.1 Data Protection, Equity, and the Accountability of Automated Law

Beyond the significant challenges of governance, legal uncertainty, and technical implementation, the adoption of blockchain in the public sector gives rise to a further set of profound risks that strike at the heart of the citizen-state relationship. These risks concern the protection of fundamental rights, the security of public infrastructure, and the preservation of equity and accountability in an age of automated decision-making. While the technology's proponents often emphasize its security and transparency, a closer examination reveals how its core properties can conflict directly with established data protection principles and undermine the very essence of the rule of law. Navigating these challenges requires moving beyond a purely technical assessment to a deeper consideration of the technology's impact on public values and constitutional safeguards.

The systemic risks are perhaps most acute in the domain of *data protection*. As previously discussed, the core feature of immutability in blockchain technology is *fundamentally at odds* with the critical data protection principles of erasure and rectification, as mandated by regulations like

the GDPR (Finck, 2018; Reddick et al., 2021). This is more than just a compliance hurdle; it represents a systemic threat to individual rights. If incorrect or sensitive personal information is permanently recorded on a distributed ledger, the process of remediation becomes legally challenging and technically fraught. The citizen is left in a perilous position, with their right to control their personal data effectively nullified by a technological design that prioritizes permanence over flexibility (Bustamante et al., 2022). Consequently, public sector implementations, particularly in Europe, have been compelled to adopt complex mitigation strategies, such as relying on *off-chain storage* for sensitive data and using advanced *pseudonymization techniques* on the chain itself, to maintain legal compliance (Bustamante et al., 2022; Fridgen et al., 2019). This necessary turn towards hybrid architectures underscores the fact that a raw, unmodified blockchain is often incompatible with legal regimes that protect fundamental human rights.

Furthermore, while distributed ledgers inherently offer redundancy and security against a single point of failure, they are by no means invulnerable to *cyber threats*. Public administrations must recognize that these systems are still susceptible to a range of generalized information system vulnerabilities as well as specific, blockchain-related attack vectors (Racsko, 2019). These risks include Sybil attacks, where an attacker creates a multitude of pseudonymous identities to gain a disproportionate influence, denial of service attacks, and the notorious *51% attack*, in which an entity controlling the majority of the network's computing power can potentially prevent new transactions from gaining confirmations or even reverse transactions (Racsko, 2019). The increasing reliance of public bodies on what are often private technological trust infrastructures creates a new and critical vulnerability: the *failure of a technical component* can severely damage the public's confidence not just in the specific service, but in the government itself (Bodó & Janssen, 2022). In this model, trust is effectively displaced from a publicly accountable institution to a complex and often opaque technical artifact, the security and resilience of which may be more fragile than is commonly assumed.

The most profound risk, however, lies in the use of *deterministic smart contracts* for public administration, which introduces serious concerns related to *equity and the accountability of automated law enforcement* (Goossens, 2021; Reddick et al., 2021). Smart contracts, governed by a rigid, rule-based "if-then" logic, are realistically only suitable for cases of *circumscribed competences that are entirely devoid of interpretive discretion* (Goossens, 2021; Komorowski et al., 2022). Yet, the vast majority of public law decisions are not simple binary operations. They frequently require the *balancing of competing interests, the exercise of interpretive judgment, and adherence to principles of good administration*, such as proportionality, due diligence, and the right to be heard, all of which are qualitative assessments that cannot be easily reduced to code (Pollicino & De Gregorio, 2021).

When rigid, automated decision-making (ADM) systems are deployed in these complex social contexts, they can act as a "black box," leading to inflexible, unequal, or discriminatory outcomes. The real-world harm of such systems has been amply demonstrated by cases where centralized ADM systems have wrongfully penalized citizens based on incomplete data or biased metrics, with devastating consequences for the individuals affected (Pollicino & De Gregorio, 2021). The *immutability and enforcement compulsion* of smart public contracts can thus transform from a theoretical virtue into a practical *"vice of technocratic rigidity"* (Kohl, 2021). When mistakes

inevitably occur or when individual circumstances change in ways the original code did not anticipate, the system's inability to adapt prevents the operation of necessary legal safety valves. The crucial possibility of administrative appeal, judicial review, or simple equitable renegotiation is foreclosed by a system designed to execute its instructions with absolute finality. This creates a brittle and often unjust form of governance, one that lacks the capacity for mercy, nuance, or the discretionary judgment that has always been a hallmark of a just legal system. The challenge for public administration is therefore not simply to implement a new technology, but to do so in a way that preserves these essential, human-centric features of the rule of law.

3.8 Conclusion: A Playbook for Legitimate Blockchain Implementation

The journey of blockchain technology from the fringes of techno-libertarian idealism to the corridors of public administration encapsulates one of the core challenges of our digital age: how to integrate powerful, decentralized technologies into centralized systems of constitutional governance without sacrificing the fundamental principles of the rule of law. This chapter has traced this journey, moving from the initial, anti-statist vision of *Lex Cryptographia* to the pragmatic reality of cautious institutionalism. The central argument that has emerged is that the successful and legitimate adoption of blockchain in the public sector is not a matter of technological inevitability, but one of deliberate and careful institutional design. It requires a fundamental shift in perspective: from viewing blockchain as a tool of radical disintermediation to seeing it as a novel institutional technology for coordination that must be carefully embedded within robust legal and organizational frameworks (Kohl, 2021).

The profound tensions between the immutable, deterministic logic of code and the discretionary, contestable nature of law are not easily resolved. As the analysis of risks has shown, a naive or technologically determinist approach can lead to systems that are not only inefficient but also inequitable, unaccountable, and fundamentally at odds with core democratic values. The evidence from pioneering jurisdictions demonstrates that the path forward lies not in replacing the state, but in co-opting the technology's distinct benefits, namely, its capacity for enhancing data integrity, auditability, and inter-agency coordination, while systematically mitigating its inherent risks through thoughtful governance. The synthesis of findings across numerous case studies and scholarly analyses leads to a set of actionable recommendations, forming a practical playbook for legislators, central digital authorities, and public agencies to ensure that blockchain implementation is successful, compliant with the rule of law, and ultimately maximizes public value.

A foundational recommendation is to adopt a *problem-driven, not technology-driven, approach*. The initiation of any blockchain project must begin not with a fascination for the technology, but with a strategic assessment of a genuine institutional coordination problem (Ølnes et al., 2017). Administrations should investigate whether the core challenge stems from a lack of trust between multiple coordinating parties or the need to replace a costly and inefficient centralized intermediary. The decision to adopt blockchain should be made only after a rigorous *suitability, scalability, and feasibility evaluation* that soberly assesses whether the technology offers a distinct

advantage over simpler, centralized alternatives (Bosch et al., 2022). This involves asking critical questions: Is the task one of circumscribed competence without the need for policy or interpretive discretion, making it suitable for a rigid smart contract (Goossens, 2021)? Or does the legality of the process require the flexibility to retroactively modify or withdraw administrative acts, making immutability a liability rather than a benefit? (Berryhill et al., 2018; Hermstrüwer, 2021).

Second, before any full-scale deployment can take place, it is imperative to *establish a clear allocation of roles, responsibilities, and liabilities* within the ecosystem. The absence of legal clarity not only creates uncertainty among stakeholders but also undermines the very trust that blockchain-based systems are intended to foster. A well-defined *legal and institutional framework* is therefore essential to delineate the duties of public authorities, private actors, and technology providers, as well as to specify the mechanisms of accountability when disputes or malfunctions arise. Only by ensuring *predictable liability structures, enforceable safeguards, and transparent governance mechanisms* can trust in the system be secured and maintained over time. In this sense, legal certainty does not simply accompany technological innovation, it is a *precondition for its legitimacy and sustainable adoption* in public governance contexts. For example, a critical challenge for blockchain adoption is the difficulty in identifying who the data controller is and assigning clear liability, a prerequisite for accountability under both public law and data protection regimes (De Hert & Kumar, 2021). In this regard, legislators and regulators must work to clearly define the roles and responsibilities of both public and private actors within the blockchain ecosystem (Goossens, 2021). For consortium models, participating public agencies must draft *joint control arrangements* through administrative agreements to specify their respective responsibilities for compliance with regulations like the GDPR (Fridgen et al., 2019). Furthermore, for the technology to move beyond the pilot phase, the legal framework must be updated to formally recognize the validity of data notarized on a blockchain and of digital signatures executed in this new environment, thereby providing the legal certainty necessary for daily operations (Bosch et al., 2022).

Third, administrations should mandate *standards-based interoperability and promote open architectures*. One of the greatest risks of ad-hoc adoption is the creation of new digital silos that are expensive to maintain and unable to communicate with one another, thereby undermining the technology's transformative potential (Ferrari, 2018). Policy efforts should therefore focus on defining international standards for security, privacy, and governance, as well as supporting the development of foundational components, such as those envisioned by the European Blockchain Service Infrastructure (EBSI), to enable scalable, cross-border public services (Alessie et al., 2019; Bosch et al., 2022). Procurement guidance should prioritize the use of *open-source software* and the adoption of layered, modular architectures to avoid the significant risk of locking the government into a single, proprietary vendor or technology (Ølnes et al., 2017; Sobolewski & Alessie, 2021).

A fourth crucial recommendation is to *strengthen audit regimes and embed legal safeguards by design*. The automation provided by blockchain and smart contracts requires robust, independent oversight mechanisms to ensure that the embedded rules uphold constitutional values. Legal safeguards must not be an afterthought but must be an integral part of the design process from its inception. This requires public agencies to conduct rigorous *Impact Assessments* to proactively analyze the risks posed by the system and ensure adherence to legal principles. Crucially,

governance cannot be limited to what is codified on-chain; it requires the establishment of strong *off-chain governance mechanisms* for dispute resolution, for providing meaningful explanations for automated decisions, and for ensuring that the right to effective judicial review is always preserved (De Filippi et al., 2020; Goossens, 2021).

Finally, and perhaps most importantly, governments must *invest in institutional capacity and foster strategic partnerships*. The evidence is clear that the greatest barriers to adoption are often organizational, not technological (Alessie et al., 2019). Public administrations must therefore focus on addressing these non-technological challenges, including organizational inertia and the incompatibility of agile development with traditional bureaucratic processes (Batubara et al., 2018). Even when technical development is outsourced, governments must *strengthen their level of in-house knowledge* to ensure they can act as an intelligent client, understanding the assumptions and decisions being coded into the technology (Berryhill et al., 2018). This necessitates partnerships with private firms and academic institutions to access expertise, coupled with a concerted effort to provide education and training for public officials to ensure they can properly run and oversee these new systems (Bosch et al., 2022; Komorowski et al., 2022).

In conclusion, the story of blockchain in the public sector is one of a radical technology being gradually domesticated to serve the enduring needs of the constitutional state. While it introduces powerful new tools for coordination and trust-building, it is not, and cannot be, a political theory capable of dismissing the role of law and democratic institutions (G'sell & Martin-Bariteau, 2022). The foundational constraints necessary for a democratic society, accountability, transparency, separation of powers, and the right to contest, were designed for traditional centralized institutions, and they must now be painstakingly adapted and enforced in this new, polycentric, and decentralized environment (De Filippi et al., 2020). The future of government blockchains will depend not on the elegance of their cryptographic proofs, but on their clear and unwavering subordination to the principles of public law. The ultimate goal must be to design and govern these systems in a manner that strengthens, rather than subverts, the constitutional commitments they are meant to serve.

4 Chapter 3: The Algorithmic Leviathan: Code, Consensus, and the Future of Organization in a Decentralized Age

4.1 Introduction and Research Context

The rise of blockchain-based organizations marks one of the most consequential experiments in private governance since the emergence of the modern corporation. From their inception, *Decentralized Autonomous Organizations (DAOs)* were envisioned as self-governing entities that could coordinate economic activity without traditional hierarchies, legal entities, or managerial intermediaries. They sought to embody, in technical form, the principles of *transparency, collective ownership, and automation*, promising to translate libertarian ideals of self-rule into programmable architectures of coordination (De Filippi & Wright, 2018; Reijers et al., 2021). Whereas the previous chapter examined how blockchain is appropriated within public governance to reinforce legitimacy and administrative transparency, this chapter turns to the *private governance domain*, exploring how blockchain enables *the creation of organizations that govern themselves through code*.

At the core of this transformation lies a profound reconfiguration of the relationship between rules, coordination, and authority. Traditional private organizations, corporations, cooperatives, or partnerships, derive their legitimacy and enforceability from legal recognition and other established, traditional rules. In contrast, DAOs claim to replace these institutional guarantees with algorithmic ones. Smart contracts and consensus mechanisms assume the functions of corporate bylaws, shareholder agreements, and even courts of arbitration, translating governance into a *rule of code*. This innovation blurs long-standing boundaries between *economic organization* and *technological infrastructure*, giving rise to what scholars describe as the “*algorithmic corporation*” (Schneider, 2019; De Filippi et al., 2024).

The promise of DAOs lies in their potential to operationalize new forms of collective action and ownership, whether in decentralized finance (MakerDAO, Uniswap), philanthropy (Bitcoin, UkraineDAO), or research collaboration (ResearchHub DAO). Yet this promise is matched by equally significant challenges. The very features that make DAOs appear autonomous, distributed governance, immutable rules, and token-based participation, also generate governance paradoxes. Decision-making frequently consolidates among large token holders, technical elites, or core developers, replicating the asymmetries DAOs were meant to eliminate (Barbureau et al., 2022; Ziolkowski et al., 2020). Moreover, the absence of clear legal personality or fiduciary accountability exposes DAO participants to regulatory uncertainty and potential liability (Finck, 2018; Reijers et al., 2021).

This chapter therefore investigates DAOs not merely as technological artifacts but as *organisational experiments*, attempts to construct self-regulating collectives that function without the scaffolding of state or corporate authority. It situates DAOs within a broader historical

trajectory of *organizational governance*, from the contractual theories of the firm to networked and polycentric forms of coordination. By doing so, it connects the technical logic of blockchain governance to the economic and legal debates that have long sought to reconcile autonomy with accountability.

Ultimately, DAOs can be read as the culmination of the decentralization project introduced in Chapter 1 and tested within the public-sector experiments discussed in Chapter 2. They represent the private-law instantiation of blockchain's ideological mission: to encode governance into the protocol itself. Yet, as this chapter will show, the attempt to achieve "governance without government" through automation re-introduces fundamental questions of trust, legitimacy, and power, questions that echo, in digital form, the very debates surrounding the corporation, the commons, and the social contract.

4.1.1 Research Statement and Questions

The principal aim of this chapter is to examine how *Decentralized Autonomous Organizations* function as laboratories for reimagining private governance in the digital age. It argues that DAOs embody a new form of *governance technology*, one that collapses the distinction between governance structure and operational mechanism. The DAO's code does not merely facilitate transactions, it *constitutes* the organization itself. This raises a central theoretical question: *can organizational order emerge from code alone, without recourse to law or hierarchical authority?*

To address this, the chapter situates DAOs within the historical evolution of governance in private law and economics. It revisits foundational theories of the firm (Coase, 1937; Jensen & Meckling, 1976), collective-action theory (Olson, 1965; Ostrom, 1990), and network governance (Powell, 1990; Rhodes, 1996), showing how blockchain's architecture operationalizes many of their normative aspirations while simultaneously challenging their underlying assumptions. Through this lens, the DAO is not an anomaly but an evolutionary step in the long-running effort to minimize agency costs and institutionalize trust among distributed actors.

Accordingly, this chapter is driven by the following research questions:

1. How do DAOs operationalize governance through technical, governance and economic mechanisms?
2. To what extent do DAOs replicate or diverge from the governance logics of traditional corporate and cooperative forms?
3. What new configurations of power and accountability arise when organizational control is embedded in code rather than law?
4. How can theories of polycentric governance and institutional economics help explain the emergent order within decentralized organizations?
5. How these novel mechanisms manifest themselves in practical applications?

By addressing these questions, the chapter positions DAOs as a pivotal site for examining how blockchain technology translates the ideological quest for decentralization into concrete mechanisms of rule, coordination, and enforcement.

4.1.2 Methodological Framework

This chapter employs a *qualitative, interdisciplinary research paradigm* to investigate the complex interplay between technology, economics, and governance in Decentralized Autonomous Organizations (DAOs). The central research question, how idealized models of decentralized governance contend with the practical realities of human coordination and power, is a question of *how* and *why*, not merely *how much*. It concerns the emergent social structures, normative conflicts, and institutional adaptations that characterize the DAO phenomenon. An interpretive approach is therefore essential, as it allows for a deep, contextualized understanding of this socially constructed reality, recognizing that a DAO's trajectory is not predetermined by its code but is shaped by the economic, social, and political environments in which it operates (De Filippi & Wright, 2018).

4.1.2.1 Research Design: Thematic Synthesis

The chapter is designed as a *comprehensive, multi-disciplinary, literature-based study* that employs a method of *thematic synthesis*. This approach is particularly well-suited for a rapidly evolving field like DAOs, where critical knowledge and empirical data are highly fragmented across disparate disciplines, including computer science, law, economics, and sociology.

The goal of this method is not to merely summarize existing work, but to *build theory by integrating findings* from these diverse fields. This involves a systematic process of identifying, analyzing, and synthesizing arguments and evidence to construct a coherent and novel theoretical framework that explains the observed patterns of DAO evolution, specifically, the central paradox of emergent centralization.

4.1.2.2 Source Selection and "Data" Collection

The primary "data" for this chapter consists of a curated body of textual sources, selected to provide a holistic, multi-faceted view of the research problem. This body of literature was systematically collected and categorized into four main types:

1. **Foundational Economic and Organizational Theory:** This includes the classical scholarship on the theory of the firm (Coase, 1937), transaction cost economics (Williamson, 1981), agency theory (Jensen & Meckling, 2019), and the governance of the

commons (Ostrom, 1990). This literature provides the classical benchmark and theoretical tools for analyzing DAOs as novel institutional forms.

2. **Foundational Technical and Conceptual Literature:** This includes the primary white papers, developer documentation, and conceptual articles that define the technical architecture and ideological vision of DAOs, such as the capabilities of smart contracts (Szabo, 1997) and the core principles of decentralization (Buterin, 2014).
3. **Socio-Legal and Governance Scholarship:** This includes the growing body of academic work critically examining algorithmic governance (Campbell-Verduyn, 2017), the "code is law" thesis and its critiques (De Filippi & Wright, 2018; DuPont, 2017), and the socio-technical nature of blockchain systems.
4. **Empirical Studies and Grey Literature:** This crucial category provides the empirical grounding for the chapter's argument. It includes quantitative studies on voter participation (Han et al., 2025) and token concentration (Barbureau et al., 2023; Fracassi et al., 2024), as well as high-quality reports from institutional bodies (e.g., World Economic Forum, 2022, 2023) and detailed analyses of major governance events (e.g., "The DAO" hack).

4.1.2.3 Method of Analysis

The analysis of this diverse literature was conducted using a three-stage thematic synthesis process:

1. **Identification of Key Concepts:** A thorough reading of all sources was undertaken to identify and code key concepts, arguments, and empirical findings (e.g., "plutocratic voting," "high coordination costs," "governance attacks," "rage quit mechanism").
2. **Organization into Descriptive Themes:** These initial codes were then collated and grouped into a hierarchical structure of related "descriptive themes" that represent recurring patterns across the literature. Examples of these themes include the persistent tension between on-chain and off-chain governance, the trade-off between decentralization and efficiency, and the vulnerability of DAOs to capture.
3. **Generation of Analytical Themes:** The final stage involved moving from description to interpretation. The descriptive themes were synthesized to generate the higher-order "analytical themes" that form the core argument of this chapter. This involved interpreting the relationships *between* the themes to build the central concept of the "governance paradox" and the overarching narrative of the gap between decentralized aspiration and emergent centralization.

This methodological framework allows the chapter to bridge the gap between technical analysis, economic theory, and socio-legal critique. By treating these disparate bodies of literature as data, the thematic synthesis makes it possible to construct a robust, theoretically grounded, and empirically informed argument about DAOs as a complex and evolving socio-technical phenomenon.

4.1.3 Contribution

This chapter makes a crucial contribution to the thesis by shifting the analysis from public law to the domain of *private governance*. Its primary methodological contribution is to bridge the often-separate fields of *technology studies* and *organizational theory*, particularly institutional economics.

Substantively, the chapter provides a critical reframing of the DAO. It moves beyond treating DAOs as mere technical phenomena and analyzes them as *novel institutional experiments*. The core argument is that DAOs do not *solve* classic economic problems of governance, such as agency costs, coordination costs, and power concentration, but rather *reconstitute them in new, digital-native forms*.

By framing DAOs as *hybrid governance regimes*, this perspective reveals the persistent and necessary tension between automated "code is law" enforcement and adaptive, human-led social coordination. This analysis demonstrates that DAOs are simultaneously *technological infrastructures* and *evolving organizational species*, thereby setting the critical foundation for Chapter 4, which will explore how these *de facto* private orders confront the *de jure* realities of the legal system.

4.1.4 Literature Review

Research on Decentralized Autonomous Organizations (DAOs) spans organizational economics, distributed computing, governance theory, and socio-legal studies. Across this interdisciplinary landscape, a shared picture emerges: DAOs aspire to overcome entrenched governance problems through cryptographic automation and decentralized decision-making, yet empirical evidence consistently reveals the persistence of coordination failures, power asymmetries, and the need for human discretion (De Filippi & Wright, 2018; DuPont, 2017; Han et al., 2025). Accordingly, scholars increasingly interpret DAOs not as a paradigm-breaking organizational form but as a continuation of established institutional dynamics mediated through new technological infrastructures (Campbell-Verduyn, 2017; Hassan & De Filippi, 2021).

The intellectual foundations of the DAO debate are grounded in organizational economics. Coase (1937) famously conceptualized the firm as a governance structure that internalizes market transactions to reduce coordination costs and uncertainty. Building on this, Williamson (1981, 1985) demonstrated how hierarchical authority emerges as an efficient institutional response to opportunism and information asymmetries. Jensen and Meckling (1976) further reframed the corporation as a nexus of contracts in which ownership and control are separated, giving rise to agency conflicts and concentrated managerial discretion. These theories provide the basis of organisational research which DAOs aim to transform. In this regard, DAOs invert these foundations by attempting to embed governance rules into executable code to reduce reliance on managerial authority (Werbach, 2018). However, the principal-agent problem persists in token-based systems, where token holders with concentrated wealth accumulate disproportionate influence over organizational outcomes (Barbereau et al., 2022; Borgogno & Martino, 2024;

Fracassi et al., 2024). Research shows that this leads to asymmetrical governance resembling corporate oligarchies rather than democratic collectives (Bellavitis et al., 2023; Tan et al., 2023). As well as the important research on network governance (Powell, 1990; Rhodes, 1996), Elinor Ostrom's (1990) work on commons and polycentric governance is also central here: institutions that rely on self-governance require robust social norms, monitoring systems, and graduated sanctions to avoid free-riding (Alston et al., 2022, 2022; Ostrom, 1990; Rozas et al., 2021). Yet DAOs' design ethos frequently overlooks these social preconditions, assuming that automation alone can supersede normative enforcement (Reijers et al., 2021; Zwitter & Hazenberg, 2020).

A second major thread in the literature focuses on blockchain architecture. Transparency, immutability, and censorship-resistance are celebrated for reducing monitoring costs and enabling verifiable enforcement (Rikken et al., 2019; Swan, 2015; Weinstein & Loftchie, 2022). Smart contracts, first conceptualized by Szabo (1997), promise reliable execution of agreements without human intermediaries (Lumineau et al., 2021). Yet several scholars argue this rigidity undermines institutional adaptability (Finck, 2018; Ziolkowski et al., 2020a). The 2016 attack on "The DAO," and the contentious Ethereum hard fork that followed, revealed that human-led exceptions are ultimately essential to organizational survival (De Filippi et al., 2024; Reijers et al., 2021). This supports Schmitt's (2005) insight that every governance system requires an authority capable of deciding in moments of exception, highlighting the limits of "code is law" positivism (Lessig, 2009). Immutability, accordingly, is not absolute but socially negotiated (L. Liu et al., 2021).

Recent research advances the view that DAOs are socio-technical governance hybrids, where algorithmic coordination coexists with human judgment. On-chain decision-making offers transparency, traceability, and automation (Kitzler et al., 2024; Y. Liu et al., 2022). Yet off-chain deliberation and expertise remain indispensable for agenda-setting, dispute resolution, and interpretation of complex proposals (DuPont, 2017; Finck, 2018). Scholars highlight the risks of informal leadership emerging among core developers, delegates, and communication gatekeepers, creating covert hierarchies that contradict decentralization ideals (Sharma et al., 2024; World Economic Forum, 2022). Empirical case studies show that DAOs increasingly rely on foundation entities, emergency councils, and multisignature wallets, which recentralize operational authority (De Filippi et al., 2023; Fischer & Valiente, 2021).

Economic research examines DAO governance as a driver of both coordination and conflict as these novel structures introduce new governance challenges while changing the older ones (D. W. Allen & Berg, 2020; Beck et al., 2018; Bohme et al., 2015; Ziolkowski et al., 2020a). For example, tokens serve as programmable bundles of rights merging ownership, governance, and speculative value with their own novel challenges (Barbereau et al., 2023; Borgogno & Martino, 2024; Schwiderowski et al., 2024). Financial incentives can undermine long-term governance by encouraging short-term speculation and exit behaviors (Bellavitis et al., 2023; Mondoh et al., 2022). Despite innovations such as Quadratic Voting and Conviction Voting (Borgogno & Martino, 2024; Faqir-Rhazoui et al., 2021), participation remains persistently low due to high gas fees, cognitive burden, and rational abstention when whale dominance renders individual votes inconsequential (De Filippi et al., 2020; Fracassi et al., 2024; Han et al., 2025; Ziolkowski et al., 2020a). This dynamic reinforces a timocratic model of governance, in which political power maps directly onto economic capital (Barbereau et al., 2023).

Finally, empirical scholarship on DAO implementations has begun to articulate distinct typologies of their practical manifestations, ranging from decentralized finance protocols to digital cooperatives and public-goods funding networks (Naudts, 2023; Weinstein & Loftchie, 2022; World Economic Forum, 2022, 2023; Ziegler & Welp, 2022). These analyses ground theoretical claims in observable organizational behavior, revealing both the innovative potential and operational constraints of DAOs in real-world environments. Importantly, case studies of governance crises, such as the bZx exploit and flash-loan-enabled attacks, demonstrate that algorithmic coordination introduces novel modes of vulnerability, allowing adversaries to strategically exploit governance rules at scale (Bannister, 2021; Commodity Futures Trading Commission, 2022a; DuPont, 2017; Lehar & Parlour, 2022). Practical examples also show that rather than eliminating traditional governance risks, DAOs relocate them into the technical architecture and incentive systems that define protocol-level decision-making.

Collectively, these scholarly insights converge on a core institutional paradox. DAOs emerged to transcend the limitations of hierarchical organization by distributing power and automating trust through code (Buterin, 2014; Hsieh et al., 2018). Yet decentralization, automation, and transparency simultaneously generate coordination rigidities, plutocracy, and sovereignty-in-crisis when exceptions arise. DAOs therefore do not signal the end of organization but illustrate how governance challenges are reconstituted in digital form. The evolution of DAOs appears less a departure from the history of governance than a new configuration of it: an experiment in institutional design where enduring socio-political dynamics remain deeply present, albeit mediated by cryptographic infrastructure and distributed economic incentives.

4.1.5 Chapter Structure and Plan

This chapter unfolds through four interrelated analytical sections, building upon the theoretical, institutional, and ideological foundations established in the preceding chapters. The analysis adopts a *multi-perspectival framework*, examining Decentralized Autonomous Organizations (DAOs) through four complementary lenses, *technology, governance, economics, and practical applications*, to provide a comprehensive understanding of their organizational logic, normative aspirations, and socio-technical implications. By engaging these perspectives in tandem, the chapter seeks to move beyond reductive narratives of decentralization, presenting DAOs instead as complex, evolving institutions situated at the intersection of code, consensus, and collective behavior.

The first analytical perspective investigates the computational architecture underpinning DAOs, examining how core blockchain features, *decentralization, transparency, immutability, and smart contract automation*, collectively enable decentralized coordination. This section dissects the technical foundations of autonomy while also exposing the embedded constraints and paradoxes of each pillar. It explores how radical transparency functions as a "double-edged sword," creating a direct conflict between public accountability and individual privacy, and how rigid immutability clashes with the need for organizational adaptability, a tension crystallized by the 2016 hack of "The DAO". The discussion also details systemic constraints, such as the "oracle problem" and the *Blockchain Trilemma*, which forces trade-offs between decentralization, security, and

scalability, situating the blockchain not merely as a ledger but as a normative *governance substrate*.

The second analytical lens focuses on how authority and decision-making are operationalized. Building on theories of network and polycentric governance, it explores the hybrid interplay between rigid *on-chain* algorithmic execution and flexible *off-chain* social coordination. This section examines voting mechanisms, from plutocratic token-weighted systems to experimental models like Quadratic Voting, while highlighting how governance processes are transformed when rules become executable. Yet, these innovations introduce new risks: the analysis identifies persistent *governance pathologies*, including the re-emergence of agency costs, chronically *low voter turnout*, and *extreme power concentration* ("whales"). This section thus treats governance not as an achieved state, but as a dynamic equilibrium between automation and community oversight, between rule by code and legitimacy from human consensus.

The third perspective connects DAO coordination to institutional and transaction-cost economics. Drawing from Coase and Jensen & Meckling, this section asks whether DAOs genuinely minimize coordination inefficiencies or merely redistribute them. It reframes DAOs as institutional competitors designed to minimize the "*costs of trust*" by substituting human intermediaries with algorithmic assurances. By analyzing *tokenomics*, the use of hybrid tokens as programmable incentives it demonstrates how blockchain embeds economic rules into organizational design. Yet, these same incentives generate path dependencies and speculative behavior, tethering governance to market volatility. Accordingly, this section reframes DAOs as *economic constitutions*, highlighting the central trade-off between decentralization and efficiency and the risks of *deep financialization* that can reinforce plutocratic power structures.

This section grounds the chapter's theory by providing a taxonomy of DAO models, analyzing them as "living laboratories" for decentralized governance. The analysis details a diverse typology based on their objectives, starting with the most prominent, *Decentralized Finance (DeFi)* DAOs like *MakerDAO* and *Uniswap*, which govern complex financial infrastructures. The survey also covers *Philanthropy DAOs* (e.g., *GitcoinDAO*) that fund public goods and (e.g., *UkraineDAO*) that act as rapid-response mechanisms for global challenges. Finally, it examines *Community and Labor DAOs* like *Raid Guild*, which use smart contracts to coordinate digital collaboration and professional services outside of traditional employment hierarchies. Each case demonstrates how DAOs function in practice, translating ideological commitments into operational design. *MakerDAO* illustrates how monetary governance can be algorithmically enforced; *Uniswap* shows the emergence of permissionless market-making; *Gitcoin* exemplifies collective funding mechanisms for public goods; and the *Optimism Collective* represents experiments with non-financial, citizenship-based governance. This section grounds theoretical insights in empirical reality, revealing both the versatility and fragility of DAO structures and their manifestations in moments of crisis and regulatory confrontation, such as the *Tornado Cash* sanctions and the canonical *hack of "The DAO"*.

Finally, the chapter concludes with the *paradox of algorithmic autonomy*, synthesizing these four perspectives into a unifying argument. DAOs, it contends, do not abolish governance; rather, they *reconstitute it* through code, consensus, and incentive alignment. The analysis reveals a persistent gap between the revolutionary rhetoric of decentralization and the empirical reality of

emergent centralization. By transforming social coordination into a programmable process, they blur the lines between infrastructure and institution, representing a *new institutional species* that merges technical architectures with normative order. This synthesis also establishes the conceptual bridge to the next chapter, where the analytical lens shifts from *governance through code* to *governance under law*. Having explored how DAOs operationalize private order, the subsequent chapter investigates how legal systems are beginning to respond to, and resist, these emerging forms of organization, examining their interaction with corporate law, liability regimes, and the legal doctrines of personhood and accountability.

4.2 The Technology Layer

Decentralized Autonomous Organizations (DAOs) represent a fundamental and potentially transformative evolution in the theory and practice of organizational structure and governance. By leveraging the unique architectural properties of blockchain technology, DAOs are pioneering a new model of human coordination that seeks to replace traditional, top-down management hierarchies with a framework that is transparent, automated, and collectively governed by a distributed community of stakeholders (Han et al., 2025). At their conceptual core, these digitally native entities embed the rules for collective action, resource allocation, and strategic decision-making directly into self-executing computer programs known as smart contracts. This foundational act of codification creates a system where governance is intended to be managed by algorithmic logic rather than by managerial decree, aspiring to build organizations that are more equitable, resilient, and transparent than their centralized predecessors (Hassan & De Filippi, 2021; Yermack, 2017). The innovative approach is not merely a technological substitution but a profound rethinking of the very nature of the firm, trust, and authority in an increasingly digital world.

4.2.1 The Principle of Decentralization

The defining characteristic and philosophical bedrock upon which the entire DAO structure is built is its profound commitment to decentralization. This principle is not simply a technical feature but the operational and ideological foundation of this new organizational paradigm (Y.-Y. Hsieh et al., 2018). A DAO is best understood as a blockchain-native system designed to empower a group of individuals, often globally dispersed and pseudonymous, to coordinate their actions and govern themselves through a shared set of rules immutably recorded on a public ledger (Hassan & De Filippi, 2021). The primary objective is to facilitate cooperation and the allocation of shared resources without relying on a central authority or the familiar hierarchies of the traditional corporate form (Y.-Y. Hsieh et al., 2018). In essence, DAOs aspire to operate without the conventional intermediaries, such as boards of directors, senior managers, or administrators, that characterize and control most modern organizations (World Economic Forum, 2022). The desire to eliminate the need for a trusted central party has been a primary driving force since the inception of blockchain technology itself, reflecting a deep-seated ambition to re-architect systems of trust (Y.-Y. Hsieh et al., 2018).

This organizational model was famously articulated by Ethereum co-founder Vitalik Buterin, who envisioned a framework of "automation at the centre, humans at the edges" (Buterin, 2014). In this construct, the core operations, financial transactions, and foundational rules are handled autonomously by smart contracts, forming an impartial and predictable algorithmic core. The human participants interact with this automated center by proposing ideas, engaging in debate, and casting votes, but they do not control the system in the traditional sense of direct managerial oversight; their influence is mediated through the very protocols that define the organization. Decentralization is operationalized by distributing control across all members, typically through the issuance of digital governance tokens that represent voting power (Han et al., 2025). Instead of a chief executive officer or a board making unilateral decisions, any member holding the requisite tokens can typically submit a formal proposal for consideration. This proposal is then subjected to a vote by the entire community of token holders. If the proposal achieves a predetermined level of consensus, such as a simple or super majority, the governing smart contract is designed to automatically execute the specified outcome without requiring approval from any intermediary, thus ensuring that power theoretically rests with the collective rather than with a single entity or a small cabal of executives.

4.2.1.1 The Dimensions and Challenges of Decentralization

However, it is crucial to recognize that decentralization is not a monolithic or binary state but rather a complex continuum with several distinct dimensions (Y.-Y. Hsieh et al., 2017). A DAO can be highly decentralized in one aspect while remaining comparatively centralized in another, and a nuanced analysis requires disaggregating these facets. The first of these is technical decentralization, which pertains to the physical and architectural resilience of the underlying blockchain network. It is often measured by the number and distribution of nodes that maintain and validate the ledger, which ensures that there is no single point of failure that could compromise the entire system (Ziolkowski et al., 2020b). Closely related is geographic decentralization, which assesses the physical distribution of the DAO's contributors and technical infrastructure across different political jurisdictions. A wide geographic spread can enhance resilience against localized regulations, censorship, or legal challenges that might threaten the organization's continuity (World Economic Forum, 2022).

Perhaps most critically, political decentralization measures how power and decision-making influence are distributed among the community's members. This dimension questions whether the organization truly reflects the collective will or if founders or early insiders retain special administrative privileges, such as "master keys" that would allow them to unilaterally alter the protocol (World Economic Forum, 2022). Achieving genuine political decentralization requires that no single entity or small group can control the organization's destiny, a principle that is fundamental to the DAO ethos (Hassan & De Filippi, 2021). This is inextricably linked to the concept of economic decentralization, which focuses on the distribution of the DAO's native governance tokens. If a small number of digital wallets hold a majority of these tokens, the organization is considered economically centralized. Such a concentration of token wealth directly compromises its political ideals, as voting power becomes a function of capital, potentially transforming a professed democracy into a functional oligarchy (World Economic Forum, 2022).

Proponents envision DAOs as a powerful instrument for profound social and economic change. By removing centralized bottlenecks and creating transparent, auditable systems of governance, they promise to democratize organizational management and foster more equitable economic outcomes (World Economic Forum, 2022). For many advocates, DAOs are seen not merely as a new corporate structure but as a potential mechanism to address deep-seated societal problems, including political oppression, economic inequality, and entrenched power asymmetries that pervade traditional institutions (Bodó, 2021; Brekke, 2021; Reijers & Coeckelbergh, 2018). Furthermore, they offer a novel method for generating and sustaining value by creating robust, peer-to-peer ecosystems that do not depend on traditional financial intermediaries for trust and execution (Y.-Y. Hsieh et al., 2017).

Despite these lofty aspirations, the practical implementation of radical decentralization presents formidable hurdles. The first and most significant is a fundamental efficiency trade-off. The process of requiring community-wide votes for a wide range of operational and strategic decisions can be incredibly slow and cumbersome, creating what economists refer to as high coordination costs. This inherent latency makes DAOs poorly suited for dynamic environments that demand rapid, time-critical decisions, and can stifle innovation by making it difficult to implement necessary software updates or emergency bug fixes in a timely manner (Finck, 2018). A second persistent challenge is the de facto concentration of power. In many prominent DAOs, governance tokens, and thus, voting power, become concentrated in the hands of a few powerful actors, such as founders, venture capital investors, and early "whale" insiders. This dynamic can lead to the emergence of quasi-oligarchic or timocratic structures, where power is derived directly from wealth, directly contradicting the ideal of broad, democratic representation and participation (Barbureau et al., 2023).

Finally, DAOs currently operate in a state of profound legal ambiguity. Their novel, decentralized, and often borderless nature makes it exceedingly difficult to fit them into existing legal frameworks for corporations, partnerships, or other recognized legal entities. In many jurisdictions, if a DAO is not formally incorporated into a recognized legal structure, it risks being treated as a "general partnership" by default (de Oliveira & Rolo, 2023). This classification carries severe implications, as it could expose every individual member to unlimited personal liability for the debts and actions of the entire organization, a risk that stands as a major deterrent to mainstream adoption. This legal uncertainty also creates immense friction when a DAO needs to interact with the traditional economic and legal world, such as signing contracts, opening a bank account, or formally hiring employees, thereby isolating it from the very systems it often seeks to improve.

4.2.2 Transparency: The Double-Edged Sword

Beyond the foundational principle of decentralization, the operational and ideological integrity of a DAO rests upon a set of interlocking technological pillars enabled by its underlying blockchain infrastructure. Among these, the commitment to transparency is paramount, representing a radical departure from the often opaque and siloed nature of traditional corporate structures. Transparency is not merely an incidental feature; it is an ideological choice and a core architectural property intended to foster unprecedented levels of trust and accountability among participants (Weinstein

& Loftchie, 2022). This principle dictates that the inner workings of the organization, from its foundational constitutional rules and day-to-day financial transactions to its formal governance decisions, are open for public inspection. While this radical openness holds the promise of a more equitable and democratic future for organizational governance, it also introduces a complex set of challenges and strategic trade-offs that the field is only beginning to navigate (De Filippi et al., 2024).

The mechanisms that facilitate this high degree of transparency are woven into the very fabric of a DAO's design, guaranteed by the public and distributed nature of its host blockchain. This technology provides what has been described as a "universal, permanent, continuous, consensus-driven, publicly auditable, redundant, record-keeping repository," where every action, vote, and transfer of funds is openly recorded and made accessible to anyone with an internet connection (Rozas et al., 2021; Swan, 2015; Weinstein & Loftchie, 2022). This creates a single, verifiable source of truth that is not controlled or mediated by any central party. This ethos of openness has deep historical roots in the digital commons, echoing the "communitarian spirit of an open-source project" that characterized the early development of foundational cryptocurrencies like Bitcoin (Wallace, 2011). Building upon this legacy, the vast majority of DAOs are governed by rules encoded in open-source software protocols and enforced by smart (Weinstein & Loftchie, 2022). Once deployed on the blockchain, these smart contracts create a "comprehensive, immutable record" of all organizational activities, which can be scrutinized by any individual possessing the requisite technical expertise, ensuring that the rules of engagement are known and cannot be covertly altered by a privileged few.

The aspirations tied to this level of systemic transparency are profound. By design, it serves as a cornerstone of DAO governance, intended to cultivate an environment of enhanced trust and accountability (De Filippi et al., 2024). The permanently open and auditable ledger creates an unambiguous audit trail, making it exceedingly difficult for any individual or group to engage in fraudulent transactions or other malicious activities without immediate and widespread detection (Weinstein & Loftchie, 2022). This capacity for real-time monitoring of all governance activities is viewed as a crucial tool for addressing regulatory concerns, such as the illicit use of insider information, by ensuring every action is traceable and attributable on the public ledger (Fracassi et al., 2024). Furthermore, this visibility aims to fundamentally reduce the conflicts of interest and moral hazard problems that plague traditional firms by overlapping the roles of principals (the owners or stakeholders) and agents (the managers), a common source of friction in corporate governance theory (Bellavitis et al., 2023).

This open-source ethos also acts as a powerful catalyst for experimentation and permissionless innovation. Because the operational code of most DAOs is publicly accessible, it provides a cost-effective framework for testing novel governance models, allowing others to learn from, build upon, and even directly challenge successful projects. The 2020 emergence of the Sushiswap protocol serves as an illustrative case study of this dynamic in action (Cryptopedia Staff, 2023). At the time, Uniswap was a pioneering decentralized exchange (DEX) governing a treasury worth billions of dollars. Because its code was open-source, a rival group of developers was able to "fork" it, a process of copying and modifying the existing code, to create a direct competitor, Sushiswap. This event, sometimes described as a "vampire attack" for its aim of draining liquidity and users from the original protocol, forced both projects into a fierce cycle of innovation to attract and retain

capital. This demonstrates how the ability to freely adapt existing code without starting from scratch dramatically lowers the barrier to entry for new competitors, accelerating the evolution of both financial and governance models in a way that is simply not possible in the closed, proprietary world of traditional corporate structures.

However, the unyielding nature of this transparency is a double-edged sword, creating a host of formidable challenges. The most significant of these is the inherent and often irreconcilable tension with individual privacy. The very features that enable accountability, the public, permanent, and immutable recording of all on-chain actions, create a lasting digital footprint. This raises profound questions about the applicability of concepts like the "right to be forgotten" in a digital context where every transaction and vote is preserved in perpetuity (Mayer-Schönberger, 2011; Rozas et al., 2021). While users typically operate through pseudonymous addresses rather than their real names, this method offers only a fragile shield. A user's entire history of on-chain activity is permanently linked to their address, which can be traced, analyzed, and, with sufficient effort and data correlation, connected to a real-world identity.

Beyond privacy, full transparency can be strategically disadvantageous in competitive environments. The case of ConstitutionDAO, which in 2021 publicly raised funds to bid on a rare copy of the U.S. Constitution, is a stark example. The public and real-time nature of its treasury size provided its competitors with perfect information, allowing a rival bidder to place a winning bid just marginally above what the DAO could afford to pay (J. Z. Tan et al., 2023). This vulnerability has sparked critical discussions around the need for strategic discretion, leading to the exploration of privacy-preserving technologies and concepts like private voting or shielded treasuries. Furthermore, there exists a crucial distinction between transparency and true legibility. While the source code of a DAO's smart contracts may be open for anyone to inspect, this does not guarantee that most community members can actually understand its complex logic or its broader implications, thereby limiting their ability to participate effectively in governance (Nabben, 2021). This can perpetuate information asymmetries between technically proficient insiders and ordinary members, leading to decision-making processes that are fundamentally opaque despite their formal openness (Campbell-Verduyn, 2018).

4.2.3 Immutability: The Unyielding Foundation

In the architecture of DAOs, the principle of transparency is inextricably bound to the technological bedrock of immutability. This core characteristic, derived directly from the blockchain, refers to the unchangeable and permanent nature of data once it has been committed to the distributed ledger. Immutability functions as the ultimate guarantor of a DAO's promises, transforming the abstract ideal of openness into a concrete, verifiable, and tamper-proof reality (Y.-Y. Hsieh et al., 2017; Rikken et al., 2019). It is the force that ensures the history of the organization cannot be retroactively altered, its foundational rules cannot be secretly bent, and its transactions cannot be erased. For DAOs, this means that the governing rules encoded in smart contracts are deployed to create a definitive and unalterable record of all organizational activity (Lumineau et al., 2021; Weinstein & Loftchie, 2022). The execution of these contracts, particularly on robust platforms like Ethereum, is effectively guaranteed, creating a system where the code

itself becomes the final arbiter (De Filippi et al., 2024). This has given rise to the powerful and often-cited maxim, "code is law," which is lauded in conjunction with the immutable and censorship-resistant characteristics of the blockchain (Borgogno & Martino, 2024). This ideal aims to substitute "trust in the secret and arbitrarily mutable activities of a private computation" with "verifiable confidence in the behavior of a generally immutable public computation" (De Filippi et al., 2024). The intended result is a new paradigm of organizational trust, enabling what scholars have termed "trustless trust" or "distributed trust," where reliance on human intermediaries is replaced by faith in the integrity of the code itself (Hoffman, 2015).

The mechanisms that enforce this powerful guarantee of permanence are multifaceted. The blockchain's data structure is designed for durability, with transactions bundled into blocks that are cryptographically sealed and then sequentially added to a growing chain, making them irrevocably linked (Weinstein & Loftchie, 2022). This chain is replicated and distributed across a vast network of participants, ensuring there is no single point of failure and making the system incredibly resilient to both malicious attacks and censorship (De Filippi et al., 2024). Security is further enhanced through the extensive use of cryptographic hashing. Each block contains not only a hash of its own transactions but also the hash of the preceding block, forging an unbreakable chronological link. Any attempt to alter data in a prior block would change its hash, which would in turn invalidate the hash of every subsequent block in the chain, immediately signaling a breach of integrity to the entire network (De Filippi et al., 2024). This process ensures the authenticity of digital records by providing an incorruptible proof of their existence at a specific point in time.

However, the rigid dogma of immutability confronts a series of profound challenges and practical limitations when applied in the real world, where human fallibility and unforeseen events are constants. The most famous and formative illustration of this tension was the 2016 hack of "The DAO," an event that forced the nascent blockchain community to grapple with the practical limits of the "code is law" ethos. When a flaw in The DAO's smart contract code was exploited by an attacker, leading to the siphoning of millions of dollars' worth of cryptocurrency, the supposedly immutable ledger had perfectly and permanently recorded a catastrophic theft (DuPont, 2017). The system operated exactly as it was coded, but the outcome was antithetical to the community's intent. In response, the community made a contentious, human-driven decision to execute a "hard fork", a radical software upgrade that effectively created a new, alternative version of the blockchain, reversing the fraudulent transactions and restoring the stolen funds (De Filippi et al., 2024).

This event starkly demonstrated that immutability is not an absolute, inherent feature of the technology but is better understood as a socially constructed norm that can be overridden by sufficient human consensus, particularly in "states of exception" (L. Liu et al., 2021). Indeed, hard forks are now understood as a primary, albeit drastic, mechanism for instituting change, adding features, and upgrading a blockchain's core protocol (Y.-Y. Hsieh et al., 2017). This reality highlights a fundamental conflict between upgradability and immutability. While a blockchain is designed for permanent data storage, absolute permanence is not always desirable. Organizations must be able to evolve, correct errors, and adapt to changing circumstances. A DAO that relies solely on its original, unchangeable code can become dangerously brittle and unable to respond to new challenges, necessitating mechanisms for upgradability that inherently compromise the principle of strict immutability (Y. Liu et al., 2023). Furthermore, the blockchain is susceptible to

the "garbage in, garbage out" problem; its permanent nature means that if erroneous or fraudulent data is entered onto the chain, it may remain there forever, extending the longevity and impact of the mistake (Ziolkowski et al., 2020a).

4.2.4 Smart Contracts: The Promise of Autonomous Execution

The engine that drives this entire paradigm of transparent, immutable, and decentralized organization is the smart contract. Smart contracts and the automation they enable are not merely ancillary features; they are the fundamental mechanisms that allow a DAO to function, transforming human agreements and organizational bylaws from passive legal documents into active, self-enforcing computer code (Han et al., 2025). This shift from human-intermediated enforcement to autonomous, algorithmic execution represents a profound rethinking of coordination and trust. By placing automated programs at the center of collaboration, DAOs aim to create systems that are more efficient, reliable, and resilient than their traditional counterparts (Hassan & De Filippi, 2021). A smart contract is a computer program deployed on a blockchain network that is designed to automatically verify and execute valid transactions when prescribed conditions are met, all without the need for a central authority or trusted third party. Though the term was first conceptualized by computer scientist Nick Szabo in 1997, it is critical to understand that smart "contracts" are not traditional legal agreements but are rather self-executing scripts whose enforcement is guaranteed by the underlying network (De Filippi et al., 2024; Szabo, 1997).

Once deployed, a smart contract's execution is automatic and occurs in a formal, non-ambiguous, and deterministic manner. This property of deterministic computation ensures that a specific input or message sent to the code will always yield the exact same outcome, allowing every node in the distributed network to independently verify the transaction's validity and thereby maintain the integrity of the shared ledger (De Filippi et al., 2024). The benefits that arise from this automated, self-executing framework are transformative for organizational design. The primary advantage is the creation of a "trustless" environment, where agreements are automatically enforced according to their predefined logic without relying on intermediaries like banks, lawyers, or escrow agents (Y. Liu et al., 2024). This directly translates into significant gains in efficiency and speed, as DAOs can dramatically improve business processes, cut administrative overhead, and shorten turnaround times for complex transactions by programmatically enforcing agreements (Zheng et al., 2020). By automating these processes and eliminating intermediaries, smart contracts can also substantially reduce the transaction costs associated with searching, monitoring, and enforcing business relationships (Lumineau et al., 2021; Vieira dos Santos, 2024). These digital contracts are the building blocks of DAOs, allowing disparate groups to pool resources into a common treasury and collectively manage it through a set of rules enshrined in code that are then automatically enforced by the blockchain infrastructure (De Filippi et al., 2024; DuPont, 2017).

4.2.4.1 *The Challenges of Codification and Rigidity*

However, the rigid and automated nature of smart contracts introduces its own series of profound challenges. A significant difficulty lies in codification. While precise, computer code inherently loses the flexibility and granularity of natural language, making it exceptionally difficult to adequately capture the nuances of human values, ethical principles, or complex relational agreements (De Filippi et al., 2023). This means that smart contracts are highly effective for routine, predictable tasks with clearly defined parameters, but they are far less suited for non-routine tasks that involve ambiguity or require adaptive judgment in the face of "unknown unknowns" (Ziolkowski et al., 2020b).

This limitation feeds into the "code is law" paradox. The purely algorithmic approach to enforcement often clashes with the reality that human roles and social relationships inevitably persist and shape the context in which the code operates (Campbell-Verduyn, 2018; Fischer & Valiente, 2021). The flawless execution of a smart contract does not guarantee that the code perfectly reflects the parties' original intentions or that it is compatible with external legal provisions, creating a potential gap between automated enforcement and social or legal legitimacy (De Filippi & Wright, 2018). Moreover, despite their automated core, DAOs often remain dependent on human intervention and off-chain mechanisms for crucial tasks like dispute resolution, strategic deliberation, and responding to unforeseen situations. This highlights that algorithmic governance is merging with, rather than fully substituting, other modes of social coordination (De Filippi et al., 2023; Ziolkowski et al., 2020b). This dependency is exemplified by the "oracle problem," also known as the "first mile/last mile problem." For a smart contract to execute based on real-world events, such as a change in a commodity price, the outcome of an election, or the completion of a physical delivery, it must receive that information from an external source. This requires trusted data feeds known as "oracles"³, which reintroduce a potential point of failure, manipulation, or centralization into an otherwise trustless system (Chainlink, 2025).

4.2.5 A Systemic Constraint: The Blockchain Trilemma

While blockchain technology offers remarkable governance affordances, its underlying mechanics reveal a persistent structural constraint commonly referred to as the Blockchain Trilemma. First articulated by Ethereum creator Vitalik Buterin, this trilemma posits that it is exceptionally difficult for a decentralized network to simultaneously achieve three critical properties: decentralization, security, and scalability (Vitalik Buterin, 2017). A network can typically optimize for only two of these attributes at the direct expense of the third. This is not a mere theoretical curiosity but the central architectural constraint that dictates the technological strategy and operational viability of every DAO, shaping its capacity for growth, participation, and real-world application.

³ Oracles are third-party services that provide blockchains and smart contracts with verified external data, such as price feeds, weather reports, or election results, bridging the gap between on-chain code and off-chain reality (Chainlink, 2025). Since blockchains cannot access external information directly, oracles serve as trusted data gateways essential for executing conditional smart contracts.

In this framework, decentralization refers to the distribution of computational power and authority across the network, ensuring there is no single point of control or failure (Mssassi & Abou El Kalam, 2024; Nakai et al., 2024). Security refers to the blockchain's ability to defend against attacks and guarantee the integrity of its ledger, a property often measured by the economic cost required for a malicious actor to successfully disrupt the network, for example, by executing a 51% attack (Antonopoulos, 2014; Nakamoto, 2008). Finally, scalability measures the network's capacity to handle a high volume of transactions efficiently, primarily assessed by its throughput (the number of transactions processed per second) and its latency (the time required for a transaction to be confirmed) (Khan et al., 2021).

The acute tension between these three properties is a direct consequence of a public blockchain's design. To achieve maximum decentralization and security, every transaction must be broadcast to and independently validated by a large and globally distributed number of nodes. As the number of nodes increases to bolster decentralization and, by extension, security, the communication and computation overhead required to reach consensus grows significantly. This process creates a severe bottleneck that inherently limits the network's processing capabilities, thus sacrificing scalability. For a DAO operating on a highly decentralized and secure Layer-1 blockchain like Ethereum, this trilemma manifests as a critical operational challenge (Faqr-Rhazoui et al., 2021). During periods of high network usage, the demand for finite block space outstrips the limited supply, leading to severe network congestion. This produces two debilitating symptoms: slow transaction speeds and exorbitant transaction fees. Confirmations for votes or other actions can take an unacceptably long time, impeding the timely execution of governance proposals. Simultaneously, users are forced into a bidding war for their transactions to be included in a block, causing transaction costs, known as "gas fees," to skyrocket (Faqr-Rhazoui et al., 2021).

This issue was the central cause of the famous Bitcoin block size debate, where many users and developers argued for increasing the block size limit in order to process more transactions and meet growing demand, while others viewed such a change as a dangerous compromise to the network's security and decentralization (Y.-Y. Hsieh et al., 2017). This ideological divide ultimately led to a contentious hard fork and the creation of a separate blockchain, Bitcoin Cash.

For DAOs, these symptoms pose an existential threat to their core principles. High gas fees can make participation in governance economically irrational for small token holders, effectively disenfranchising a large portion of the community and concentrating decision-making power among wealthier stakeholders who can afford the costs (Han et al., 2025). This directly undermines the ideal of political decentralization. Furthermore, it can render any DAO operations that rely on frequent or low-value transactions completely unviable from a business perspective, severely limiting their potential use cases. The urgent need to overcome this structural bottleneck has driven the blockchain ecosystem's intense focus on *scaling innovations*, particularly *Layer 2 solutions*⁴ such as *rollups*, *sidechains*, and *state channels*, which aim to offload transaction

⁴ *Layer 2 scaling solutions* refer to secondary frameworks built atop a base blockchain to improve transaction efficiency without compromising its security (Kraken, 2024). *Rollups* aggregate multiple transactions off-chain and post them to the main chain in compressed form, reducing congestion while maintaining verifiability. *Sidechains* are independent blockchains interoperable with the main chain, allowing assets to move between networks with faster and cheaper transactions. *State channels*, by contrast, enable participants to conduct multiple off-chain interactions privately, recording only the final outcome on the main chain to minimize on-chain activity.

processing from the main chain while preserving the core principles of decentralization and security (Kraken, 2024).

4.3 The Governance Layer

Governance has long been theorized as unfolding through three archetypal coordination modes, *hierarchies, markets, and networks*, each mobilizing distinct logics of authority, incentives, and information (Thompson, 1991). Hierarchies centralize decision rights and rely on command, rules, and administrative oversight; markets coordinate through prices, competition, and contracts; networks, by contrast, privilege horizontal ties, reciprocity, and iterative collaboration among interdependent actors (Rhodes, 1996).

Powell's (1990) *theory of network governance* provides a particularly valuable interpretive bridge for understanding this third mode. Unlike markets or hierarchies, which are structured around formal contracts or top-down authority, networks derive stability and coordination from *relational trust, shared norms, and mutual monitoring*. Cooperation within networks depends on the cultivation of reputation, reciprocity, and the maintenance of social capital rather than coercive enforcement or price competition. Information flows freely across nodes, and power is diffused through patterns of communication and interdependence rather than consolidated in managerial hierarchies. The network, therefore, represents a distinctive organizational form that relies on endogenous mechanisms of accountability, trust, transparency, and ongoing interaction, to sustain order and coherence (Powell, 1990).

This conceptualization becomes especially pertinent in the digital age. Over the last half-century, structural shifts in technology and political economy have elevated the salience of networks as dominant forms of organization and coordination. Building on the *theory of the firm* (Coase, 2012) and *transaction cost economics* (Williamson, 1981), scholars anticipated that advances in information and communications technologies would erode the costs of peer-to-peer coordination, rebalancing the long-standing hierarchy–market trade-off in favor of more distributed forms of organizing (DiMaggio et al., 2001; Malone et al., 1987).

This transformation culminates in the “network society,” structured by the *space of flows* and *timeless time*, where flexible, scalable, and resilient networks reprogram legacy institutions and redistribute “programming” and “switching” power across connected nodes (Castells & Cardoso, 1996). Within this social morphology, value creation and governance are increasingly determined by informational exchange and digital interconnectivity rather than bureaucratic command or market price.

Seen through this lens, *DAOs* can be interpreted as *automated instantiations of network governance*. They transpose Powell's sociological insights into a computational register: reputation systems, cryptographic transparency, and consensus mechanisms collectively perform the coordinating functions once achieved by trust and mutual accountability. DAOs thus encode the cooperative logic of network governance into technological infrastructures, demonstrating how the relational mechanisms of trust and reciprocity can be operationalized through algorithms,

distributed ledgers, and self-executing smart contracts. DAOs promise, *network-native governance*, membership that is open and global; decision rights mediated by tokens or credentials; treasuries and rules administered by smart contracts; and procedural transparency by default (Buterin, 2014; Hassan & De Filippi, 2021; Yermack, 2017). Conceptually, they fuse market-like incentives (tokenized stakes and price signals), network logics (peer production, modular collaboration, forkability), and elements of hierarchical coordination (delegates, core teams, emergency councils). As such, DAOs are best understood as hybrids that operationalize network governance *in code* while remaining embedded in legal, economic, and social environments that they cannot fully automate. In this respect, the development of DAOs highlight the fundamental shift from human-centric management hierarchies and toward an operational model where rules, decision-making processes, and organizational execution are primarily encoded in computer software and automated in a networked structure (Campbell-Verduyn, 2017). This computationally enforced network structure is designed to reduce the need for centralized human intermediaries, thereby fostering organizations intended to be more transparent, efficient, and directly controlled by their members. However, while DAOs are often idealized as fully automated, self-governing entities that entirely remove the fallibility of human discretion, the practical reality is far more complex and nuanced.

However, the underlying code that forms the constitution of a DAO is rarely flawless; it is a product of human creation and thus requires continuous upgrades and development to adapt to new challenges and opportunities. This essential maintenance and evolution cannot occur in a vacuum; it necessitates persistent human involvement, which in turn demands the establishment of robust and well-defined governance structures to guide that intervention. Consequently, the governance mechanisms developed within DAOs are not merely technical afterthoughts but direct responses to the core challenge of coordination that plagues any collective enterprise: how does a distributed network of individuals, who may not know or personally trust one another, collectively make binding decisions that advance their shared objectives?

Instead of relying on the familiar institutional apparatus of boards of directors, executive management teams, and the external enforcement of legal contracts, DAOs leverage a novel combination of cryptographic tools, primarily smart contracts, alongside innovative consensus mechanisms and voting structures to govern their operations. By their very nature, DAOs are internet-native entities that operate entirely on blockchain software, conceived as a new form of collective governance tailored specifically for online communities (Faqr-Rhazoui et al., 2021; Weinstein & Loftchie, 2022). This digitalization represents a much deeper integration of code as the primary medium of governance itself, transforming abstract bylaws into active, self-enforcing protocols. This new model introduces what can be described as "governance by technology" or "algorithmic governance," a system where the inherent characteristics of the blockchain, such as immutability, transparency, and automated execution, profoundly influence and structure human behavior (Campbell-Verduyn, 2017). This is a practical manifestation of Lawrence Lessig's seminal argument that "code is law," which posits that the architecture of a software environment itself functions as a powerful form of regulation, creating distinct incentives and constraints that guide user activities (Lessig, 2009). Within the context of a DAO, the encoded rules are not mere suggestions; they are the unyielding physics of the organizational environment.

However, DAOs are not merely collections of encoded rules operating through automated execution. While the automation of rules and decision-making through smart contracts (*on-chain governance*) plays a central role in their operation, *human involvement* remains indispensable. *Off-chain governance*, encompassing deliberation, coordination, and interpretation, continues to provide the flexibility, judgment, and social legitimacy that purely algorithmic systems cannot achieve.

4.3.1 The Duality of DAO Governance: On-Chain and Off-Chain

One of the most distinctive characteristics of DAOs lies in their hybrid form of governance, which combines *automated execution* with *human discretion*. Although DAOs are often portrayed as self-governing entities capable of operating entirely through code, in practice their governance unfolds across two intertwined layers: *on-chain* and *off-chain*. The on-chain layer encompasses all processes that are executed and enforced automatically by smart contracts, ranging from proposal voting and fund allocation to protocol upgrades, ensuring transparency, immutability, and procedural certainty. The off-chain layer, by contrast, represents the social, deliberative, and interpretive dimension of governance, where human actors debate, coordinate, and negotiate before decisions are ultimately formalized on the blockchain (De Filippi et al., 2024; Reijers et al., 2021).

This duality reveals a central paradox of decentralized governance. While the on-chain environment promises objectivity and autonomy by “outsourcing trust” to code, it remains dependent on the off-chain sphere to supply interpretation, adaptability, and legitimacy. Rules written in smart contracts can determine *what* happens, but they cannot determine *why* or *how* a collective should respond to unforeseen circumstances. The DAO, therefore, is not a purely technical organization but a *socio-technical system*, where governance emerges through the continuous interaction between deterministic algorithms and contingent human judgment.

Understanding this interplay is essential for analyzing the real functioning and limitations of DAOs. The following sections explore this dual architecture in depth: first by examining the logic of *automated execution* and *human intervention*, then by analyzing *on-chain governance* as the constitutional layer of code, and finally by turning to *off-chain governance* as the social layer that sustains adaptability, consensus, and legitimacy in decentralized communities.

4.3.1.1 The Interplay Between the Algorithms and Humans

A key consequence of this code-based framework is the high degree of automated execution it enables. Once a DAO’s purpose and its operational rules are established and encoded into its governing smart contracts, there is theoretically less need for direct human involvement in its routine operations. In this idealized model, the organization can autonomously perform a wide range of tasks, such as distributing funds from its treasury, managing contributor payments through smart contract-based agreements, providing digital services, or even coordinating with other software protocols and Internet of Things devices, all without the explicit, moment-to-moment

approval of a human manager (El Faqir et al., 2020). Human intervention is primarily reserved for moments of constitutional change, where a modification to the fundamental rules is proposed and must be deliberated and voted upon by the collective of token holders (Weinstein & Loftchie, 2022). This automated framework is what facilitates the reduction of intermediaries, enabling direct peer-to-peer interaction and bypassing many of the centralized "trust actors", including governments, lawyers, banks, and corporate management, that are essential to the functioning of the traditional economy (Weinstein & Loftchie, 2022). However, it is crucial to recognize that this digitally native framework is not a monolithic, self-contained system. Effective governance in these organizations involves a complex and continuous interplay between technologically enforced rules and human-led deliberation, a distinction best understood as the difference between on-chain and off-chain governance (De Filippi et al., 2024). While DAOs strive for a model where all significant rules and decisions are executed directly on the blockchain in a transparent and automated fashion, they almost invariably depend on significant off-chain elements to function (DuPont, 2017). Reflecting this dualistic nature, most mature DAOs operate as hybrids, strategically mixing decentralized, on-chain procedures with targeted forms of centralization where effective coordination, security, or legal compliance demands it (Y. Liu et al., 2023; Reijers et al., 2021; World Economic Forum, 2022).

4.3.1.2 On-Chain Governance: Code as Constitution

On-chain governance denotes the rule systems and decision-making procedures that are embedded directly into a protocol and its associated smart contracts. In this model, permissible actions are specified *ex ante* and are executed deterministically by the network once predefined conditions are met, a process that displaces many of the oversight and execution roles traditionally held by corporate directors or administrators (Fischer & Valiente, 2021; Weinstein & Loftchie, 2022). Because enforcement is performed by code rather than by human intermediaries, bypassing these rules is structurally difficult, if not impossible; once a transaction satisfies a contract's predicates, network validators approve it and the state of the protocol transitions accordingly (De Filippi et al., 2024; Reijers et al., 2021). The infrastructure itself simultaneously defines the field of permissible interactions and supplies the execution environment for collective choices.

This architectural design has profound functional consequences. First, many management routines become self-executing. Processes such as conditional fund transfers, token vesting schedules, or time-locked protocol upgrades can occur automatically without the intervention of human gatekeepers (Fracassi et al., 2024; Han et al., 2025; Wright, 2021). Second, the immutable nature of the ledger renders all governance decisions publicly auditable. Every proposal, vote tally, and final outcome is permanently recorded on-chain, which dramatically enhances transparency and enables robust post-hoc accountability (Kitzler et al., 2024; Y. Liu et al., 2022). Proponents of on-chain governance emphasize its high degree of implementation fidelity; the tight integration of voting and execution removes any reliance on trusted third parties to enact ratified decisions, thereby reducing the principal-agent frictions that plague traditional organizations (Han et al., 2025). However, these benefits come with characteristic constraints. Code is precise but not easily adaptive, and deterministic rules struggle to handle exceptions, ambiguity, and non-routine tasks that require nuanced human judgment (Y. Liu et al., 2022; Ziolkowski et al., 2020b). Furthermore,

participation is explicitly costed, as every on-chain vote is a transaction subject to variable network fees, which can spike during periods of congestion and suppress turnout, especially among small token holders (Han et al., 2025; Kitzler et al., 2024).

4.3.1.3 Off-Chain Governance: The Social Layer

In contrast, off-chain governance encompasses the deliberative, organizational, and legal processes that shape a DAO but occur outside the blockchain's direct execution layer. This includes a wide range of human-centered activities, from agenda-setting and debate in community forums like Discourse, technical coordination on platforms like GitHub, and informal consensus-building in chat applications like Discord, to stakeholder bargaining and interactions with external legal and regulatory entities (Finck, 2018; Y. Liu et al., 2023). Because these activities are centered on human communication and social negotiation, they can tolerate ambiguity, support iterative problem-solving, and respond more quickly to "unknown unknowns", such as novel bugs, security exploits, or regulatory shocks, that the code could not have anticipated (Y. Liu et al., 2023).

These off-chain processes are indispensable for several reasons. They supply crucial flexibility, allowing communities to triage incidents, reach provisional agreements, and prototype solutions before formalizing changes through a binding on-chain vote (A. Zwitter & Hazenberg, 2020a). They also improve access and reduce costs; the development of gas-less signaling tools such as Snapshot has dramatically lowered participation frictions, enabling broader, low-stakes community polling to gauge sentiment prior to a costly and irreversible on-chain action (Han et al., 2025; Kitzler et al., 2024). Finally, the off-chain layer is where legal compliance is mediated. Formal agreements, financial disclosures, and vendor contracts are managed off-chain to align the DAO's activities with national laws, and these forums offer avenues for dispute resolution that code alone cannot provide (Finck, 2018; Ziolkowski et al., 2020b). However, these processes introduce their own governance risks. A strong reliance on trusted coordinators, such as core development teams or foundation members during the off-chain processes, can recentralize influence and enable "personal sovereignty" dynamics in which powerful individuals disproportionately shape outcomes (Han et al., 2025; Reijers et al., 2021).

Empirically, DAOs blend both modes of governance, with a clear maturation trend toward a form of *constitutionalization*. This involves treating the on-chain code as a *living constitution* that not only governs day-to-day routines but also encodes the rules for changing those rules, while pairing those technical protocols with clear, natural-language charters, emergency procedures, and defined fiduciary standards for stewards who operate critical functions (De Filippi et al., 2023; Ziolkowski et al., 2020b).

An important point must be emphasized at this stage. Crises tend to reveal the *boundary conditions of algorithmic authority*. The hack of *The DAO* demonstrated that when the stakes become existential, communities instinctively fall back on *off-chain social consensus* to legitimize extraordinary on-chain measures such as hard forks (DuPont, 2017). This exposes the presence of a *latent "network sovereign"*, a concentration of authority among influential developers, validators, and major stakeholders who can steer the community during periods of instability (De

Filippi et al., 2024; Reijers et al., 2021; Ziolkowski et al., 2020b). In such moments, blockchain governance mirrors the dynamics of *constitutional crises* familiar from political history. As Rossiter observed, the power to declare and manage an emergency seldom resides with the collective itself but rather with those possessing the operational means to act (Rossiter, 2017). The pattern recalls the fate of the *Roman Republic*, where repeated declarations of emergency during times of tumult gradually eroded republican checks and balances. Figures like *Julius Caesar*⁵ exploited these exceptional circumstances to consolidate personal authority, ultimately transforming temporary crisis powers into a *permanent monopoly of control* and marking the transition from republic to empire.

Similarly, in blockchain ecosystems, moments of existential disruption, such as the DAO hack, expose the paradox that systems built to eliminate centralized power can, under the pressure of crisis, recreate it. The capacity to intervene, suspend rules, and “decide on the exception,” to use Schmitt’s (2005) phrase, becomes concentrated in a few hands, effectively replicating the very asymmetries of authority that decentralization was meant to dissolve (Schmitt, 2005). These episodes reveal that sovereignty in decentralized systems does not vanish but instead shifts location, from the state to the network, and within the network, from the collective to those who can act decisively when code alone cannot.

Reijers (2021) interprets the *DAO Hack* and subsequent hard fork through the lens of *Carl Schmitt’s* critique of *Hans Kelsen’s* legal positivism (Kelsen, 2017; Reijers et al., 2021; Schmitt, 2005). Kelsen’s formalism, grounded in the idea that legal validity flows from the hierarchical structure of norms, leaves little room for exceptions; yet Schmitt famously countered that every legal order ultimately rests on a *decision* that suspends the norm in moments of existential crisis, the *state of exception*. In the blockchain context, the decision to intervene through a hard fork represents precisely such a suspension of the “code is law” principle, where social consensus overrides algorithmic determinism to preserve the integrity of the community. As Rossiter observed in his study of constitutional emergencies, the authority to declare and manage a state of exception rarely belongs to the collective itself but to those who possess the operational means to act, mirroring how, in Ethereum’s case, developers and foundation leaders exercised de facto sovereignty by deciding to rewrite history in response to the DAO Hack (Rossiter, 2017).

This analogy highlights that blockchain governance, much like constitutional democracy, must grapple with the tension between *normative closure* and *situational flexibility*. The assertion that the code of the blockchain should be paramount and exceptionless reflects a form of “blockchain positivism” analogous to *Kelsen’s legal purity* (Reijers et al., 2021). Yet, as the DAO crisis illustrated, rigid adherence to this ideal becomes untenable when faced with catastrophic failure or fraud. Schmitt’s insight that every system requires an authority capable of acting outside the norm resonates powerfully here: DAOs, for all their decentralization, depend on actors who can exercise

⁵ Julius Caesar exploited a period of political crisis and weakness in the late Roman Republic to amass unprecedented personal power. After defeating his rivals, notably Pompey, he was appointed dictator first for a limited term and later for life. This centralization of power effectively subordinated the Senate and republican institutions to his control, creating a near-autocratic rule. He held multiple powers including permanent tribunician powers and censorial powers, which allowed him to dominate the Senate and political machinery, shifting the republic’s balance toward personal rule.

discretion in exceptional circumstances. Consequently, blockchain systems continue to operate in a *prolonged state of exception*, where the boundaries of code-based sovereignty are repeatedly negotiated through acts of collective interpretation and extra-procedural decision-making. Far from invalidating decentralization, these episodes reveal that legitimacy in DAOs is a *multi-layered process*, emerging from the interplay of technical rules, social consensus, and the capacity to adapt law-like code to the unpredictable realities of governance (Reijers et al., 2021; Wang et al., 2019)

4.3.2 Consensus and Voting Mechanisms

The operational core that makes automated execution and decentralized agreement possible is the consensus mechanism, which serves as the fundamental process by which a distributed network of actors collectively agrees on a single, shared version of truth. In the absence of a central authority to decree the official state of the ledger, these mechanisms provide the algorithmic foundation necessary to synchronize all participants, ensuring they see the same chronological order of transactions and that the integrity of the on-chain record is maintained (De Filippi et al., 2024; El Faqr et al., 2020). This function is not merely technical; it is the sociotechnical engine that transforms the abstract principles of decentralization and immutability into a functional reality. By mobilizing algorithms to validate transactions, consensus mechanisms create a "confidence machine" that replaces reliance on traditional intermediaries with verifiable trust in the network itself (Campbell-Verduyn, 2018; De Filippi et al., 2020). Their primary purpose is to provide the automated enforcement that underpins the "code is law" ethos, guaranteeing that the terms of a smart contract will be executed deterministically once initiated, thereby mitigating opportunism and ensuring a predictable environment for coordination (Y.-Y. Hsieh et al., 2018; Lumineau et al., 2021).

4.3.2.1 Consensus Mechanisms

The landscape of consensus mechanisms has evolved significantly, moving from initial models designed primarily to secure the underlying blockchain ledger to more sophisticated systems tailored for the complex and nuanced challenges of organizational governance. The genesis of blockchain consensus lies with Proof-of-Work (PoW), the mechanism famously implemented by Bitcoin and initially by Ethereum. In a PoW system, network participants, known as "miners," are required to expend significant computational energy to solve a complex cryptographic puzzle. The first miner to find the solution earns the right to add the next block of transactions to the chain and is rewarded with a grant of the network's native cryptocurrency (Beck et al., 2018; Gervais et al., 2016). This process is deliberately resource-intensive, creating a form of "unforgeable scarcity" that secures the network against malicious attacks by making it prohibitively expensive for any single actor to alter the blockchain's history (Y.-Y. Hsieh et al., 2018). However, PoW has drawn substantial and sustained criticism for its immense energy consumption, which contributes significantly to environmental degradation (De Filippi et al., 2024; Pelt et al., 2021), and for its

tendency to foster the centralization of mining power in large-scale industrial operations located in regions with cheaper electricity (Finck, 2018).

In response to these significant drawbacks, Proof-of-Stake (PoS) emerged as a more energy-efficient alternative, eventually adopted by the Ethereum network. In a PoS system, the right to validate new blocks and earn transaction fees is assigned to participants not based on computational power, but on the amount of cryptocurrency they hold and are willing to "stake" as collateral (Pelt et al., 2021). This model fundamentally realigns incentives with the long-term health and security of the network; validators who act maliciously or fail to perform their duties risk having their staked capital "slashed," or confiscated by the protocol (De Filippi et al., 2024; Y.-Y. Hsieh et al., 2017). While PoS effectively addresses the environmental concerns associated with PoW, it introduces new and pressing governance challenges. By tying validation rights directly to capital, it risks creating a plutocratic system where "whales", large token holders, can exert disproportionate influence over the network's operation, potentially undermining the core ideal of decentralization (Barbereau et al., 2022; Faqir-Rhazoui et al., 2021).

4.3.2.2 DAO Voting Models: From Plutocracy to Experimentation

While PoW and PoS are crucial for securing the ledger, the internal governance of DAOs requires more nuanced mechanisms specifically designed for collective decision-making. The most prevalent model for DAO voting is the "one token, one vote" system, which directly mirrors the "one share, one vote" structure of traditional corporate governance (Han et al., 2025). In this arrangement, a member's voting power is directly proportional to their token holdings, implementing what is a fundamentally plutocratic system of governance (De Filippi et al., 2024; Reijers et al., 2021). While straightforward to implement, this approach is highly susceptible to the concentration of power, enabling wealthy actors to dominate decision-making and potentially advance their own interests at the expense of the wider community. This dynamic has spurred extensive experimentation with alternative voting models designed to foster more equitable, effective, and resilient governance.

One such innovation is Quadratic Voting (QV), a mechanism which allows participants not only to vote for or against a proposal but also to express the intensity of their preferences. This is achieved by making the cost for submitting multiple votes for a single proposal increase quadratically, meaning a cost of n^2 tokens for n votes (Borgogno & Martino, 2024). This design aims to give more weight to proposals that garner broad but moderate support from many individuals rather than those with intensely strong support from a wealthy few, thereby mitigating the outsized influence of whales (De Filippi et al., 2024; World Economic Forum, 2023). Similarly, Conviction Voting introduces a temporal dimension to the decision-making process. In this model, individuals can express a continuous preference over time; the longer a member allocates their tokens to a specific proposal, the more "conviction" that proposal accrues, which in turn increases its probability of passing (Bellavitis et al., 2023; Faqir-Rhazoui et al., 2021). This favors proposals with sustained, long-term support over those that could be pushed through quickly by a temporary majority.

To address the persistent challenges of voter apathy and the difficulty of scaling decision-making in large DAOs, mechanisms like Holographic Consensus and Liquid Democracy have been developed. Holographic Consensus, pioneered by the DAOstack platform, utilizes a prediction market to help filter and prioritize proposals; the community stakes tokens on initiatives they believe will succeed, which directs collective attention to the most promising ideas and allows them to pass with a relative, rather than absolute, majority (Faqr-Rhazoui et al., 2021). Liquid Democracy, also known as delegated voting, provides a flexible hybrid between direct and representative democracy. It allows members to either vote directly on a proposal or delegate their voting power to a trusted expert on a given topic, while crucially retaining the ability to revoke that delegation or resume direct voting at any time (Sharma et al., 2024). In practice, however, this can still lead to a concentration of influence among a few key delegates (J. Z. Tan et al., 2023).

Finally, recognizing the inherent risks of immutable code and the potential for a majority to tyrannize a minority, the "Rage Quit" mechanism emerged as a critical safeguard for minority rights, particularly in the aftermath of The DAO hack crisis (El Faqr et al., 2020; Weinstein & Loftchie, 2022). Popularized by Moloch DAO and its many derivatives, this feature allows any member who disagrees with a passed proposal to exit the DAO and withdraw their proportional share of the treasury assets before that proposal is executed (Faqr-Rhazoui et al., 2021). This creates a powerful game-theoretic incentive for consensus-building and compromise, as a contentious decision that harms a minority faction could trigger a mass exodus of members and capital, thereby ensuring the organization remains accountable to all its stakeholders. This continuous experimentation underscores that consensus in DAOs is not a solved problem but a dynamic field of institutional design, constantly negotiating the deep tensions between algorithmic efficiency and the messy realities of human coordination.

4.3.3 Governance Pathologies and Legitimacy Crisis

Despite the novelty of their architectural design and the sophistication of their coordination mechanisms, DAOs remain susceptible to many of the fundamental challenges that have long afflicted traditional organizations. These challenges span technical, governance, and ethical dimensions, revealing that technological innovation alone does not eliminate enduring institutional vulnerabilities.

4.3.3.1 *Inherited Challenges: Agency, Information, and Coordination*

The foundation of modern corporate governance rests on agency theory, which conceptualizes the perennial problem arising from the separation of ownership and control within firms (Fama & Jensen, 1983; Jensen & Meckling, 2019). In this model, shareholders, acting as principals, delegate managerial authority to agents, such as executives and board members, whose personal risk appetites, time horizons, and private incentives may diverge significantly from their own. The result is a structural vulnerability to opportunistic behavior, whether in the form of shirking responsibilities, rent extraction, or self-dealing, which generates measurable agency costs that traditional governance systems attempt to mitigate through a complex combination of legal

contracts, monitoring mechanisms, and carefully structured incentives (Borgogno & Martino, 2024; Connelly et al., 2010; Y.-Y. Hsieh et al., 2017).

In the context of DAOs, this classic problem reappears in a novel guise. The "agents" in this new framework are not salaried managers but are instead the disproportionately powerful token holders, colloquially known as whales, alongside the core developers who often retain significant influence. Their concentrated ownership or technical knowledge allows them to sway outcomes in token-weighted voting systems, often in ways that may conflict with the dispersed interests of smaller participants (Han et al., 2025). The conflict that agency theory diagnosed in traditional firms as a divergence between owners and managers is thus manifested in DAOs as a divergence between minority and majority stakeholders within pseudonymous, digitally mediated communities. The persistence of these conflicts of interest underscores a critical insight: decentralization does not, by itself, dissolve governance pathologies; rather, it reconfigures their lines of contestation from the boardroom to the blockchain.

A second classical governance challenge that endures, and is often magnified, within DAOs concerns information asymmetries. In traditional firms, informational gaps between insiders (management) and outsiders (shareholders) limit the potential for efficient monitoring and informed participation. In decentralized networks, these asymmetries are frequently amplified by the profound technical sophistication of blockchain systems and the inherent opacity of their underlying code to non-specialists. Early debates surrounding Bitcoin, for instance, often remained narrowly technocratic, a focus that tended to obscure the technology's broader societal and distributive implications (Campbell-Verduyn, 2017). Similarly, in DAOs, the complexity of the distributed architecture and the sheer volume of on-chain data make it exceedingly difficult for most participants to assemble and interpret relevant information, creating high barriers to meaningful participation (Fracassi et al., 2024). Consequently, only a small cadre of technically skilled insiders may be able to fully parse the intricacies of smart contracts or the economic implications of governance proposals, creating implicit hierarchies of knowledge that undermine the ideal of radically inclusive participation these communities often espouse (Borgogno & Martino, 2024; Campbell-Verduyn, 2018).

4.3.3.2 Digital-Native Pathologies: Rigidity and Governance Attacks

Alongside these inherited challenges, DAOs introduce a new set of governance problems that are specific to their digital-native constitution. A distinctive pathology is their structural rigidity. Because their foundational rules are codified in immutable or semi-immutable smart contracts, even minor adjustments can require a laborious process of community deliberation, formal voting, and technical recoding (Weinstein & Loftchie, 2022). This architecture, while promoting determinism and predictability, significantly hampers adaptability. In times of crisis, such as the discovery of a critical security bug, the need to organize a community-wide vote consumes precious time, leaving the protocol exposed to opportunistic exploitation (Naudts, 2023). The immutability that is prized as a virtue thus becomes a liability when organizations must pivot or adapt to dynamic market conditions (Bellavitis et al., 2023). The "code is law" mantra perfectly

illustrates this paradox; while algorithmic authority promises autonomy, crises reveal its incompleteness, as exceptions and emergencies invariably require human intervention and judgment that code alone cannot provide (Rozas et al., 2021; Ziolkowski et al., 2020b). As previously explained, this dynamic has been examined in detail through the lens of Reijers and classical legal theory, particularly the debate between Kelsen and Schmitt. Kelsen's legal positivism, grounded in the primacy of rules, parallels the blockchain ideal of "code is law", where validity derives from adherence to pre-established norms (Reijers et al., 2021).. Yet, as Schmitt argued, every legal order ultimately depends on the capacity to act in a state of exception, to suspend the norm when circumstances demand it (Schmitt, 2005). In the context of DAOs, crises such as The DAO Hack reveal precisely this tension: despite the aspiration toward rule-based autonomy, communities inevitably rely on human discretion and off-chain decision-making to restore order. Thus, blockchain governance cannot function as pure automation; it remains contingent on social consensus and the presence of actors capable of exercising judgment when the code proves insufficient (Reijers et al., 2021).

Perhaps the most novel and acute vulnerabilities are governance attacks, which arise from the unique combination of token-based voting and permissionless financial markets. A governance attack occurs when a malicious actor amasses sufficient voting power to pass self-serving proposals, often with the express purpose of seizing control of the organization's treasury. The most infamous instance remains the hack of The DAO in June 2016, when an attacker exploited a recursive call bug not to break the rules, but to use the rules of the smart contract against itself to siphon roughly one-third of the project's funds (Han et al., 2025). The fallout was so severe that it required the aforementioned controversial hard fork of the Ethereum blockchain, an event which split the community and exposed the fragility of "immutability" in practice (DuPont, 2017).

Other significant examples of DAO hacks include the 2020 attack on the bZx protocol, where a flash loan was exploited to manipulate governance votes and drain funds, and the 2021 Poly Network hack, one of the largest DeFi thefts, which involved exploiting vulnerabilities related to multi-chain token swaps, although the hacker later returned most of the funds (Bannister, 2021; Chavez-Dreyfuss, 2021). These attacks underscore the ongoing risks of governance manipulation and complex smart contract vulnerabilities inherent in decentralized autonomous organizations.

Subsequent attacks have evolved in sophistication, moving beyond exploiting code bugs to manipulating the governance process itself. Vote-buying through simple token accumulation or through more complex financial instruments like collateralized or flash loans enables attackers to engineer temporary super-majorities. Flash loans, which allow a user to borrow a massive amount of cryptocurrency for the duration of a single transaction block, are a particularly potent weapon. In a notable 2022 incident, an attacker used a flash loan to borrow a vast quantity of governance tokens for the Beanstalk protocol. With this temporarily acquired voting power, the attacker passed a malicious proposal that transferred \$182 million from the project's treasury to their own wallet, all within a single transaction, before repaying the loan (Lehar & Parlour, 2022; Mondoh et al., 2022). Other threats include Sybil attacks, which involve the multiplication of pseudonymous identities to manipulate voting outcomes, a tactic seen in repeated reorganizations of the Ethereum Classic blockchain (Han et al., 2025; Rikken et al., 2019). These episodes demonstrate that DAO vulnerabilities are not purely technical but are deeply socio-technical, emerging from the complex

interaction of economic incentives, code design, and the dynamics of digital asset markets (L. Liu et al., 2021). This analysis highlights both the continuities and novelties of governance challenges in DAOs, where age-old problems of agency and power are refracted through a new technological lens, creating a distinct and hazardous risk landscape.

4.3.3.3 Ethical Challenges and the Crisis of Legitimacy

These persistent pathologies give rise to a more profound set of ethical and social challenges that strike at the very legitimacy of the DAO model as a viable alternative to traditional forms of governance. The emergence of these organizations foregrounds fundamental questions about the relationship between code, human judgment, and authority. The 2016 crisis of The DAO, for instance, was not merely a technical or financial failure; it was a deeply ethical one. It demonstrated the immense difficulty of delegating final authority to pre-programmed, self-executing systems. When vulnerabilities in its smart contract code were exploited, the community was forced to confront the unsettling reality that algorithmic rules alone could not provide a satisfactory or just resolution (Campbell-Verduyn, 2018). This episode crystallized the core ethical terrain of decentralized governance: whether human judgment can, or indeed should, be subordinated to code, and under what circumstances it must retain the power to override algorithmic authority (DuPont, 2017).

This notion of algorithmic authority suggests that software protocols, by embedding and enforcing rules, begin to resemble a new kind of legal or normative regime in their own right. Yet this claim raises deeply uncomfortable questions: to what extent can legitimacy and accountability truly be vested in inanimate code, and where must responsibility ultimately remain anchored in human agency? (Nabben, 2021). This places a significant moral and social responsibility on the designers and developers who build these systems, as their architectural choices determine not only technical parameters but also the very digital infrastructures that shape community life, with profound consequences for individual autonomy and collective control. In this context, legitimacy plays a constitutive role in sustaining DAOs, which must rely on voluntary participation rather than coercive enforcement to survive (Campbell-Verduyn, 2018; De Filippi et al., 2024). For members, DAOs are very easy to leave comparing to companies thanks to the easiness and speed crypto-tokens provide. Because of that to ensure that participants remain loyal to a DAO, they must perceive its rules and decisions as fair, responsive, and, crucially, amendable. This requires governance processes that can iterate and self-correct, rather than rigidly insisting on the infallibility of the "code is law" ethos (De Filippi et al., 2023).

Drawing from political theory, this challenge can be parsed into the distinct concepts of input and output legitimacy. Input legitimacy derives from inclusiveness and fairness in the participation process, whether community members feel their concerns are represented and their voices can meaningfully influence outcomes (Campbell-Verduyn, 2018; De Filippi et al., 2024). In DAOs, this dimension is consistently undermined by the prevalence of plutocratic, token-weighted voting systems, the opacity of highly technical discussions, and persistently low participation rates, which collectively risk excluding large swathes of the community from meaningful engagement (Barbureau et al., 2022). By contrast, output legitimacy concerns

whether governance produces effective and timely outcomes. Here too, DAOs often struggle, as decentralized decision-making can be slow and contentious, leading some observers to value the efficiency and agility of more centralized organizations more highly, especially in competitive global markets (Y.-Y. Hsieh et al., 2017; Wright, 2021).

4.3.3.4 *Low Turnout and Power Concentration*

Perhaps the most persistent and visible symptom of this legitimacy problem is chronically low voter turnout. Empirical studies reveal that, on average, fewer than one-quarter of eligible token holders participate in governance votes. The disparity is even more stark when distinguishing between informal and binding decisions; only about 24% of holders cast votes in off-chain Snapshot proposals, while binding on-chain participation hovers around a mere 11% (Han et al., 2025). Even in moments of existential crisis, turnout has remained minimal; fewer than 10% of coin holders took part in the critical *carbonvote* that followed The DAO hack (Finck, 2018). This pattern of disengagement raises significant legitimacy concerns. When only a small minority of stakeholders participate, motivated actors with modest absolute stakes can shape outcomes disproportionately, increasing the risks of capture and eroding trust in the fairness of the system (Finck, 2018).

This pattern is driven by several structural factors. High gas fees are a major deterrent, as casting a single on-chain vote is a transaction that can cost anywhere from ten to over one hundred dollars during periods of peak network congestion, making routine participation prohibitively expensive for smaller holders (Han et al., 2025). Furthermore, the time and complexity involved in evaluating often lengthy and highly technical proposals create significant cognitive burdens, leading to voter fatigue and rational disengagement (Bellavitis et al., 2023; Y.-Y. Hsieh et al., 2017). Finally, when small holders believe their votes will not alter outcomes, especially in the presence of dominant whales, they rationally choose to abstain, a dynamic that further exacerbates inequality and discourages the participation of minority voices (Barbureau et al., 2023; Han et al., 2025).

This leads to the critical tension that exists between the decentralized ethos of DAOs and the actual concentration of power within them. To quantify this gap, researchers widely employ the Gini coefficient to measure inequality in the distribution of governance tokens, and the empirical findings are stark (Barbureau et al., 2023; Fritsch et al., 2024; Juodis et al., 2024). An analysis of Ethereum's own governance revealed that just ten individuals were responsible for proposing 68% of all implemented Core EIPs, the most critical protocol upgrades (Fracassi et al., 2024). Studies of major Decentralized Finance (DeFi) protocols have found that distributions of voting rights are consistently and highly concentrated. An examination of nine major projects, including Uniswap and Aave, found that fewer than one hundred addresses control more than 50% of the voting power in nearly all cases (Barbureau et al., 2023). In AAVE, just 53 addresses collectively controlled more than half of the active token supply, while at certain points, no more than five wallets held over 50% of UMA's active governance tokens. Even in Yearn Finance, a project known for a "fair launch" strategy intended to widely distribute tokens, a mere 21 accounts held over 50% of the active supply (Barbureau et al., 2023). These figures underscore a substantial

centralization risk and the threat of "governance capture," where a small, coordinated group could, in principle, determine outcomes unilaterally, undermining both the decentralization narrative and the long-term resilience of the system.

4.3.4 Polycentric Governance and Digital Commons

Building on this analysis of internal governance structures, DAOs can also be understood through a broader theoretical lens, specifically, *Elinor Ostrom's theory of commons governance and polycentric institutional design*.

Elinor Ostrom's theory of *polycentric governance* provides a foundational framework for understanding how collective systems can sustain order without centralized authority. In her seminal work *Governing the Commons* (1990), Ostrom rejected the binary opposition between state control and market privatization, demonstrating that communities are capable of self-organizing to manage shared resources effectively (Ostrom, 1990). The work identified a set of design principles, clearly defined boundaries, participatory rule-making, graduated sanctions, and local conflict-resolution mechanisms, that allow multiple centers of decision-making to coexist and coordinate. Crucially, polycentric systems operate through overlapping jurisdictions that interact, compete, and cooperate, producing a dynamic equilibrium rather than a singular hierarchy. This model of decentralized yet structured governance has become a touchstone for scholars seeking to explain emergent forms of coordination in complex socio-technical environments.

A growing body of research applies this framework to the study of DAOs (Alston et al., 2022; De Filippi et al., 2023; Rozas et al., 2021). Scholars such as Rozas et al. (2021), De Filippi et al. (2023) and Allen et al. (2019) argue that DAOs can be understood as *digital commons*, where the shared resource is not a forest, fishery, or irrigation system, but the protocol itself, its *codebase*, *token economy*, and *governance structure* (D. W. Allen et al., 2019; De Filippi et al., 2023; Rozas et al., 2021). In these digital ecosystems, coordination emerges from the interplay between algorithmic enforcement and communal negotiation, producing a new type of institutional arrangement that blends technical precision with social adaptability.

Within this framework, *smart contracts* function as *the hard layer* of governance. They encode the rules of interaction, define permissible actions, and automatically enforce compliance. Alongside them, *social governance mechanisms*, off-chain discussions, signaling processes, and proposal deliberations, operate as *the soft layer*, enabling contextual interpretation and collective adjustment. The coexistence of these layers exemplifies what De Filippi et al. (2024) describe as "*polycentric governance by code*": a configuration in which technical, economic, and social centers of authority overlap and interact dynamically (De Filippi et al., 2024). Governance in DAOs thus becomes a distributed process of mutual calibration between algorithmic logic and human consensus, yielding a system that is at once rule-bound and adaptable.

However, polycentricity within DAOs can be inherently fragile. While the code enforces certain norms with mechanical precision, it cannot resolve disputes or interpret intent. The absence of

recognized legal frameworks for adjudication leaves DAO participants exposed to uncertainty and opportunism. Moreover, despite the rhetoric of decentralization, decision-making often recentralizes around key off-chain actors such as *core developers*, *protocol foundations*, and *treasury councils*, whose technical authority or control over resources gives them disproportionate influence. These concentrations of power reveal a persistent *duality between algorithmic autonomy and social dependence*. DAOs, rather than transcending governance, reconstitute its enduring dilemmas, those of agency, legitimacy, and accountability, within a digital substrate.

Viewed through this Ostromian lens, DAOs are not anarchic collectives but *polycentric governance systems* that extend the principles of commons management into algorithmic infrastructures. They demonstrate that cooperation and order can emerge without centralized control, provided that rule-making, monitoring, and enforcement are distributed across multiple, interlocking centers of authority. Yet, their sustainability depends on achieving balance: between formal, immutable rules and flexible, community-driven adaptation; between transparency and inclusivity; between the efficiency of automation and the responsiveness of human judgment. In this sense, DAOs serve as *institutional experiments in algorithmic commons management*, both fulfilling and testing Ostrom's vision in the digital age. They reveal that the promise of decentralization lies not in the abolition of governance, but in its reconfiguration through layered systems of code, consensus, and collective action.

This polycentric lens thus situates DAOs not merely as novel governance tools, but as emerging institutional competitors, new actors in the ecology of global coordination that blend algorithmic control with communal rule-making.

4.3.5 A New Institutional Competitor

The journey of DAOs represents a profound and ongoing experiment in the future of organization and governance. While they introduce powerful new tools for coordination and collective action, they do not escape the classic challenges of agency, information, and power that have shaped human institutions for centuries. Instead, they reframe these enduring problems in a digital-native context, while simultaneously creating novel vulnerabilities tied to the deterministic yet brittle nature of code. The governance of DAOs is thus defined by a deep and persistent negotiation between the rigid logic of automated systems and the adaptive, nuanced, and often unpredictable needs of human collaboration. The empirical evidence of low participation and high power concentration reveals a significant gap between their decentralized aspirations and their plutocratic reality, posing a serious challenge to their long-term legitimacy and sustainability. Moving forward, the success of this organizational form will depend not on a blind faith in technology, but on the ability of their communities to design more inclusive, resilient, and ethically robust governance structures that can effectively bridge the divide between the power of code and the wisdom of the collective.

4.4 The Economic Logic of Decentralized Organizations

The analysis of Decentralized Autonomous Organizations from an incentives and economic perspective reveals the profound ways in which these entities challenge and reconfigure conventional economic theories of organization and coordination. DAOs are not merely technological artifacts but are better understood as institutional innovations that re-architect how resources, information, and trust are organized in productive enterprises. Their design choices around incentive structures, often mediated by cryptographically secured tokens, create novel and complex trade-offs between the competing virtues of decentralization, efficiency, equity, and the ever-present risk of power concentration. These tensions situate DAOs as experimental laboratories for rethinking some of the foundational assumptions in organizational economics and corporate governance. Unlike traditional firms, cooperatives, or clubs, DAOs rely on blockchain-based infrastructures to reduce dependence on trust in human intermediaries, codify rules through transparent smart contracts, and enable direct, often borderless, participation by stakeholders (Han et al., 2025; Hassan & De Filippi, 2021). Yet, the economic rationale of DAOs is not a story of unambiguous improvement; while they promise to reduce certain agency costs, transaction costs, and the hazards of information asymmetry, they simultaneously create new forms of hold-up costs, collective action problems, and plutocratic risks.

From the perspective of organizational economics, DAOs emerge as institutional competitors to markets, hierarchies, and other forms of collective action. The seminal theory of the firm, articulated by Ronald Coase, explains that firms exist to minimize the transaction costs associated with using the open market, such as the costs of discovering prices, negotiating contracts, and monitoring performance (Coase, 2012). DAOs, in turn, can be interpreted as a new organizational technology designed to minimize a different, though related, category of costs, the "costs of trust" (Davidson et al., 2018). By embedding rules into transparent, auditable, and self-executing smart contracts, DAOs promise to substitute fallible interpersonal trust with verifiable machine-based assurances (M. Becker & Bodó, 2021b). This framing suggests that DAOs represent neither a complete break from nor a simple continuation of traditional firms. Instead, they expand the menu of institutional choices available to society. Where firms aggregate resources and coordinate labor through hierarchical authority and legally enforceable contracts, DAOs aspire to achieve similar ends through distributed incentives and algorithmic governance (Y. Hsieh & Vergne, 2023).

4.4.1 Reconfiguring Transaction Costs, Agency Costs, and Property Rights

Transaction cost economics, which highlights the frictions inherent in market exchange, provides a powerful lens for analyzing this shift (Williamson, 1981). DAOs alter the calculus of these costs by automating large portions of contracting and enforcement. For instance, rules for allocating voting rights or distributing revenues can be written directly into code, reducing the need for costly human monitoring and legal oversight. Yet, DAOs do not eliminate transaction costs altogether; rather, they alter their composition. On one hand, they can dramatically reduce *ex-ante* contracting costs, as once the rules are encoded and deployed, their execution becomes automatic and predictable. On the other hand, they may significantly increase *ex-post* coordination costs, particularly when bugs, unforeseen contingencies, or governance disputes arise that were not

anticipated in the original code (Beck et al., 2018). The 2016 hack of The DAO exemplifies this dilemma perfectly. What was intended as a fully self-executing contract required an unprecedented and costly process of off-chain social coordination to resolve, ultimately leading to a hard fork of the entire Ethereum blockchain (DuPont, 2017). Thus, DAOs substitute the costs and risks of trusting people with the costs and risks of trusting code, which, while different, are by no means trivial.

This reconfiguration of organizational structure also has profound implications for agency theory. As previously discussed, traditional firms suffer from the classic separation of ownership and control, which necessitates elaborate systems to align the interests of principals and agents. DAOs appear to blur or even collapse these distinctions. Token holders may simultaneously act as users, investors, and governors, which theoretically should create a powerful alignment of incentives (Han et al., 2025). However, the reality reveals the persistence of old agency problems and the creation of new ones. Large token holders, or "whales," can disproportionately influence decisions to their own benefit, replicating or even intensifying the very conflicts of interest that DAOs seek to overcome (Sharma et al., 2024). In some cases, developers retain privileged administrative controls, undermining the rhetoric of decentralization and reintroducing a clear principal-agent dynamic (Barbereau et al., 2023).

Furthermore, the operational logic of DAOs introduces significant *hold-up costs*. Because rules are encoded into rigid smart contracts, they can be exceptionally difficult and costly to change. This inflexibility means that a DAO can become a hostage to its own outdated or flawed code, unable to renegotiate terms or adapt to changing market conditions without contentious and high-stakes interventions like a hard fork (L. Liu et al., 2021). These hold-up dynamics demonstrate that DAOs, like traditional firms, must constantly negotiate a difficult balance between the predictability that comes from rigid rules and the adaptability required to survive in a dynamic environment.

Finally, the economic logic of DAOs can be powerfully illuminated through the lens of property rights theory, which posits that efficient investment and resource allocation require clarity in asset ownership and control (Riordan & Williamson, 1985). While traditionally applied to physical assets and corporate equity, this framework extends naturally to DAOs, which are fundamentally organized around the creation and management of digital assets, namely, their native tokens, their underlying code, and the data they generate. The governance tokens that are central to most DAOs embody a novel and programmable bundle of rights, which can include residual claims on the value generated by the protocol, voting rights over proposed changes, and specific usage or access rights for the services the DAO provides (Wang et al., 2019).

The true innovation lies in the unprecedented flexibility DAOs have in the bundling and unbundling of these rights. In traditional corporations, equity is a relatively standardized instrument that typically combines residual financial claims with voting rights in a fixed manner. In DAOs, by contrast, the rights associated with a token can be meticulously designed and customized through its governing smart contract. This enables a vast field of experimentation in institutional design that is simply not possible within conventional legal and financial frameworks (Borgogno & Martino, 2024). For example, a DAO can issue tokens that grant access to a platform's services but confer no voting rights, while another might implement

complex voting models like quadratic or conviction voting to deliberately sever the linear relationship between capital ownership and political influence (J. Z. Tan et al., 2023). These varied designs illustrate how DAOs operationalize property rights theory in new ways, embedding the very structure of governance directly into programmable, digitally native assets.

4.4.2 Tokenomics and the Architecture of Incentives

At the heart of a DAO's economic system lies the token, a programmable and transferable digital asset that functions as the primary medium for coordinating behavior, distributing value, and allocating control. These tokens are hybrid economic instruments that blur traditional financial categories. They can simultaneously embody the characteristics of equity, by granting holders a claim on the long-term value and success of the project; currency, by serving as a means of exchange within the DAO's ecosystem; and property, by providing specific access or usage rights to a platform's functionalities (Wang et al., 2019). This multifaceted nature allows tokens to function as governance rights, payment instruments, and community identifiers all at once. Unlike shares in a corporation, which are highly standardized and bound by established legal frameworks, tokens are infinitely customizable. A DAO can encode differentiated voting weights, automated revenue-sharing formulas, or conditional access restrictions directly into the token's smart contract. This makes tokenomics, the formal study and design of token-based economic systems, both an emerging economic science and a critical practice of institutional engineering (Y. Liu et al., 2023). A sound token model must carefully integrate incentives for both human capital (the effort, expertise, and reputation of contributors) and monetary capital (the financial resources provided by investors) to achieve a sustainable alignment among all stakeholders (Wang et al., 2019).

4.4.2.1 *Monetary Incentives*

DAOs deploy a range of monetary incentives to attract capital, reward participation, and ensure the long-term sustainability of their ecosystems. These pecuniary incentives typically fall into two broad categories. The first includes direct rewards for network operation, such as the transaction fees or block rewards paid to node operators or validators who secure the underlying blockchain infrastructure (Y. Liu et al., 2022). The second, and more common, incentive is the potential for market-driven appreciation in the token's value. Contributors and investors who hold a DAO's governance or utility tokens are often motivated by the prospect of significant financial returns if the project gains traction and its token becomes more valuable. This mechanism mirrors the logic of equity appreciation in traditional startups, although the token markets are often far more volatile and speculative. While these monetary incentives are powerful tools for attracting participation at scale, they also tether DAOs to the unpredictable dynamics of the broader crypto-asset markets. A participant's behavior can shift rapidly with price volatility, exposing DAOs to the risks of short-term speculation rather than the stability of long-term community-building.

4.4.2.2 Other Incentives

However, not all incentives within these systems are financial. DAOs also leverage a potent array of non-pecuniary rewards, such as reputation, community recognition, enhanced visibility, and social influence (Beck et al., 2018). Reputation systems, whether formalized through on-chain attestations and credentials or developed informally through community memory and social platforms, help to distinguish high-quality contributors and signal trustworthiness. In many DAOs, this accumulation of social standing and symbolic capital acts as a powerful motivator, complementing or even superseding monetary returns for certain participants. This dual-incentive system reflects broader findings in organizational economics, which have long recognized that humans are not purely rational maximizers of wealth but are also deeply motivated by a sense of recognition, belonging, and purpose (Ostrom, 1990). DAOs effectively harness these social dynamics to sustain volunteer labor, knowledge-sharing, and collective problem-solving in environments where traditional employment contracts are absent. Moreover, DAOs elevate the *role and visibility of reputation* as a central mechanism of trust. Because *pseudonymity* is intrinsic to most decentralized systems, participants are often recognized not by their real-world identities but by the *reputational capital* they accumulate through their contributions, interactions, and track records within the community. In such environments, reputation effectively substitutes for identity, serving as the primary basis for credibility and influence.

A striking feature of DAO economies is the gamification of labor. Early blockchain systems, particularly Bitcoin, introduced a model where users were rewarded with tokens for contributing computational power to validate transactions, a process that has been likened to a "game" where participants maximize self-interest in pursuit of a collective outcome (Maurer et al., 2013). DAOs extend this logic by embedding gamified incentive schemes into a broader range of organizational functions. Contributors may earn digital badges, non-fungible tokens (NFTs), or enhanced governance privileges for completing specific tasks, participating in votes, or successfully recruiting new members. These gamified mechanisms help to sustain engagement and direct effort in contexts where traditional managerial oversight is absent.

This leads to a fundamental shift in the organization of labor itself, creating models that resemble but also diverge from the open-source software movement (Ljungberg, 2000). Contributors are often self-selected, globally distributed, and pseudonymous. Compensation takes innovative forms, such as streaming payments that deliver wages in a continuous, real-time flow, or bounty-based systems that offer one-off payments for the completion of specific, well-defined tasks (J. Z. Tan et al., 2023; World Economic Forum, 2022). While these flexible models significantly lower barriers to participation, they also create new forms of precarity and uncertainty. Defining fair compensation for ongoing, complex, or creative contributions remains an unsolved challenge; for example, coding bounties may work well for discrete bug fixes but fail to account for the long-term, often invisible, labor of maintaining and upgrading complex software protocols (J. Z. Tan et al., 2023). Moreover, this novel organization of labor complicates fundamental questions of employment status, taxation, and labor rights. Without clear contractual relationships, contributors often occupy an ambiguous legal position, being neither formal employees nor fully independent contractors. This ambiguity has profound implications for labor law and the economic stability of contributors.

4.4.3 Economic Trade-Offs and Systemic Challenges

While the architecture of incentives in DAOs is innovative, its implementation in the real world gives rise to a series of fundamental economic trade-offs and systemic challenges. These issues reveal the inherent tensions between the ideological goals of decentralization and the pragmatic demands of operational efficiency, market stability, and equitable governance. The economic reality of DAOs is not one of seamless, automated harmony, but a complex landscape of coordination costs, speculative pressures, and emergent power structures.

One of the central dilemmas facing every DAO is the trade-off between decentralization and efficiency. Economic and organizational theory predicts that more decentralized decision-making structures, while potentially more inclusive and representative, are also more time-consuming and prone to coordination failures (Y.-Y. Hsieh et al., 2017). In DAOs, where significant proposals often require community-wide deliberation and voting, the decision-making process can become sluggish and inefficient. Emergency software updates, critical bug fixes, or swift strategic pivots in response to market changes may stall due to low voter turnout, lengthy debate periods, or the sheer logistical difficulty of mobilizing a globally distributed community. This inherent inefficiency stands in stark contrast to the agility of centralized firms, where executives can often act swiftly and decisively. Consequently, many investors and market participants perceive highly decentralized governance not as an asset, but as a potential liability, fearing it hampers innovation and the ability to compete effectively (Y.-Y. Hsieh et al., 2017). This tension forces DAOs to constantly seek a balance between their core principle of inclusivity and the practical need for functionality, often leading them to adopt hybrid governance models that delegate certain powers to smaller, more agile committees while retaining ultimate oversight for the broader community.

Contrary to the initial expectation that automation would drastically reduce organizational overhead, DAOs often exhibit surprisingly high governance costs. While smart contracts can automate the execution of decisions, significant costs arise in the human-centric processes that precede any on-chain action. The negotiation of complex proposals, the technical labor of writing and auditing secure code, and the social effort required to resolve disputes all consume substantial time and resources (Beck et al., 2018). The very rigidity of smart contracts can amplify these costs; once deployed, code is difficult and expensive to change, meaning that any unforeseen event or flaw can lead to costly workarounds or contentious, high-stakes interventions like a hard fork. This creates a paradox where a system designed to minimize the coordination costs of human interaction may, in practice, generate entirely new layers of governance expenses (Fischer & Valiente, 2021). This reality underscores the status of DAOs as complex sociotechnical systems, where technological efficiency can never fully substitute for the difficult and expensive work of human coordination and consensus-building.

Perhaps the most significant set of challenges stems from the deep financialization of DAO governance. As the tokens that grant voting rights are also tradable financial assets, DAOs are inextricably linked to the volatile dynamics of crypto-asset markets. They are increasingly used as collective investment platforms, pooling capital to pursue ventures ranging from venture capital to the collection of digital art (World Economic Forum, 2022). Investment DAOs like MetaCartel Ventures and FlamingoDAO demonstrate the remarkable speed with which these communities can

raise and deploy significant funds. Yet, this financialization exposes DAOs to extreme market volatility. Token prices can swing wildly, affecting not only the value of a DAO's treasury but also the incentives of its participants. Members whose primary motivation is financial may quickly exit during market downturns, leaving the DAO vulnerable to instability and a loss of human capital (Ziolkowski et al., 2020a).

This has led many critics to contend that DAOs often function less as democratic communities and more as high-risk speculative vehicles (Borgogno & Martino, 2024). In such an environment, participants may be incentivized to prioritize short-term token price appreciation over the long-term health and sustainability of the organization, undermining the promise of durable, community-led governance. This critique resonates with the cautionary tale of The DAO from 2016. Marketed as a revolutionary decentralized venture fund, its structure encouraged rapid, widespread investment, but it ultimately collapsed following a smart contract exploit that resulted in the loss of millions of dollars in investor funds. The event underscored the profound dangers of treating DAOs primarily as speculative instruments without first establishing robust safeguards and mature governance processes (DuPont, 2017).

Ultimately, the financialized nature of governance tokens often leads back to a significant concentration of voting power, creating a direct conflict with the ethos of decentralization. Because tokens can be freely bought and traded on secondary markets, they often accumulate in the hands of a few large investors or "whales." This can create systems that resemble plutocracies (the form of rule by wealth) and timocracies (the form of rule by property), in which political power is directly proportional to capital ownership (Barbereau et al., 2023; Sharma et al., 2024). This concentration fundamentally undermines the democratic aspirations of the DAO model. Whales can dominate votes, steer treasury allocations to their own benefit, and create an environment where smaller holders feel their participation is futile, thereby suppressing engagement and re-creating the very agency problems that DAOs were intended to solve (Han et al., 2025). As the empirical data on token distribution demonstrates, this is not a theoretical risk but a present reality in many of the largest DAOs, challenging the narrative of these entities as inherently democratizing institutions.

From an economic standpoint, DAOs thus embody both radical promise and profound contradictions. They leverage programmable tokens to align incentives, reduce certain transaction costs, and reconfigure property rights, yet they simultaneously generate new agency problems, high coordination costs, and significant speculative risks. The tension between decentralization and efficiency runs through every facet of DAO economics, forcing a constant negotiation between ideological purity and pragmatic survival. Ultimately, DAOs highlight the limits of purely technological solutions to longstanding economic dilemmas. They represent an ongoing experiment in institutional design, an effort to reconcile the complex realities of human collective action with the formal logic of algorithmic coordination.

4.5 The Practical Manifestations of Decentralized Organizations

While the preceding analysis of governance and economics reveals the internal logic and theoretical challenges of DAOs, the manifestation perspective turns to how these abstract designs are translated into real-world organizational forms. DAOs are not merely conceptual frameworks; they manifest as living platforms, dynamic communities, and ongoing governance experiments that interact with, and often challenge, existing social, economic, and legal systems. Their applications are increasingly diverse, ranging from the high-stakes world of decentralized finance to the aspirational domain of humanitarian aid, and from experiments in digital democracy to the creation of cooperative labor platforms. This perspective underscores the dual role that DAOs currently play in the institutional landscape: they are at once competitors to traditional institutions, such as firms, cooperatives, and governments, and laboratories of experimentation, where novel governance models are tested in real time with tangible stakes. The very process of their manifestation illuminates both the profound strengths and the persistent weaknesses of the model: its unprecedented ability to rapidly pool resources, its deep reliance on programmable yet rigid rules, its inherent exposure to market speculation, and its unresolved tension with existing legal frameworks.

DAOs can be understood as novel institutional forms that compete directly with established organizational structures like firms, clubs, cooperatives, and markets (Borgogno & Martino, 2024; Ziolkowski et al., 2020a). In Coasian terms, they represent an alternative solution to the fundamental economic problem of allocating resources and coordinating human effort. Where markets coordinate through price signals and firms coordinate through hierarchical authority, DAOs attempt to coordinate through algorithmic rules and tokenized incentives. This positioning situates DAOs within the broader field of organizational pluralism. Rather than completely replacing traditional forms, they introduce new possibilities for hybrid arrangements, where established institutions begin to adopt DAO-like mechanisms for transparency or stakeholder engagement, or where DAOs incorporate features of traditional firms, such as off-chain legal wrappers like foundations or limited liability companies. This blending illustrates how institutional competition often results in adaptation and integration rather than outright displacement.

4.5.1 DAO Typologies

The practical objectives of DAOs vary widely, and this diversity shapes their manifestation. Some are oriented primarily toward wealth creation, such as investment DAOs that pool capital to make speculative ventures in new crypto projects or digital assets. Others focus on community building, emphasizing the development of a collective identity, shared culture, and the practice of governance experimentation itself. A third, and increasingly common, category pursues finite, well-defined goals, after which the DAO may dissolve. The most famous example, ConstitutionDAO, formed with the singular purpose of purchasing a rare copy of the U.S. Constitution at auction (World Economic Forum, 2022). This typological diversity complicates any attempt to generalize about DAOs. An investment DAO like MetaCartel Ventures, a community DAO like Friends with Benefits, and a finite-purpose DAO like ConstitutionDAO all

share structural similarities, such as token-based governance and a reliance on smart contracts, but they differ profoundly in their purpose, social dynamics, and measures of success. The existence of finite-goal DAOs in particular demonstrates how blockchain technology enables a new organizational archetype: the "pop-up organization" that can emerge, raise millions of dollars in a matter of days, pursue a narrowly defined task, and then dissolve, thereby dramatically reducing the temporal and administrative friction of collective action.

DAOs also manifest their objectives through distinct means of coordination, primarily focused on organizing people, deploying capital, and managing (World Economic Forum, 2023). They provide powerful coordination frameworks for globally distributed communities that may never meet physically, using governance tokens and communication platforms like Discord to facilitate deliberation and decision-making across borders. They have proven exceptionally effective at deploying capital, pooling resources into shared treasuries with a speed and scale that is difficult to replicate through traditional means. Finally, some DAOs use their token economies to manage ongoing activities, such as software development or protocol maintenance, functioning like open-source communities but with the added dimension of direct financialization.

A rapidly growing and socially significant manifestation is the Impact DAO, defined as any DAO that explicitly pursues a positive social or environmental outcome (World Economic Forum, 2023). Examples range from climate-focused DAOs funding carbon removal projects to education DAOs supporting open-access research and knowledge creation. A notable early case demonstrating the potential of the underlying technology was the United Nations World Food Programme (WFP), which piloted the use of the Ethereum blockchain to distribute vouchers for refugee aid (Lumineau et al., 2021). Though not a DAO in the formal sense, the project demonstrated how blockchain-based systems can enhance transparency, reduce corruption, and empower beneficiaries in humanitarian contexts. Impact DAOs extend this model, applying decentralized governance principles to mobilize and allocate resources for the social good. Their emergence challenges the stereotype of blockchain technology as a purely speculative domain. By embedding purpose-driven objectives into their organizational DNA, these DAOs align with the long traditions of social enterprises and cooperatives, albeit with a novel programmable infrastructure. Still, they face a central dilemma: how to reconcile their altruistic missions with the realities of tokenized incentives that often attract speculative, rather than mission-aligned, capital.

Interestingly, empirical studies suggest a correlation between a DAO's stated purpose and its effective level of decentralization. Impact and community-oriented DAOs often demonstrate broader token distribution and lower Gini coefficients, suggesting higher levels of decentralization in their governance structures. By contrast, infrastructure DAOs (such as those managing core blockchain protocols) and investment DAOs tend to exhibit a greater concentration of voting power among fewer actors (Sharma et al., 2024). This correlation reveals an institutional paradox: the DAOs that most closely embody the decentralized and democratic ethos in their missions also tend to reflect it in their structures, while those pursuing purely financial returns frequently drift toward de facto centralization. This observation challenges simplistic narratives of DAOs as being inherently democratic or decentralized, emphasizing instead that the degree of decentralization is not a uniform technical property but a variable that reflects an organization's core purpose and sectoral context.

4.5.2 DAO Platforms as Enabling Infrastructure

The practical manifestation and proliferation of DAOs depend heavily on the development of platform architectures that significantly lower the barriers to entry for communities wishing to form their own decentralized organizations. While it is technically possible for a team of developers to build a DAO entirely from scratch by writing a unique suite of smart contracts, most communities rely on pre-existing frameworks that provide standardized and audited modules for core functions like governance, treasury management, and voting. These platforms, often themselves governed as DAOs, serve as critical meta-institutions that enable the rapid growth of the broader DAO ecosystem (Faqr-Rhazoui et al., 2021). Among the most prominent are Aragon, DAOstack, and DAOhaus, each of which offers a distinct philosophical and technical approach to balancing the competing demands of flexibility, usability, and decentralization. It is crucial to recognize that these frameworks are not neutral technical scaffolds; they actively shape the governance culture of the DAOs built upon them by embedding their own assumptions about decision-making, voting models, and organizational structure.

Aragon stands as one of the earliest and most influential DAO deployment platforms, designed with the ambitious goal of allowing users to create a wide range of internet-native entities, from open-source software projects to digitally native corporations and nonprofits (Aragon, n.d.). Its architecture, based on a modular operating system called aragonOS, defines stakeholder rights and privileges as a set of interoperable smart contracts (Wang et al., 2019). The core design principle of Aragon is modularity, enabling communities to select and plug in different governance applications, such as various voting systems, token issuance controllers, or even third-party dispute resolution services, that can be tailored to their specific needs. This flexibility is intended to foster innovation by allowing for a wide range of experimentation. However, it also creates significant challenges for systematic analysis, as the activity across the thousands of Aragon-based DAOs is diverse and fragmented (Faqr-Rhazoui et al., 2021). Furthermore, the very flexibility of the system can create vulnerabilities; the ability to install custom modules means that well-resourced or technically sophisticated actors could potentially design and pass governance systems that entrench their own control.

Another example, DAOhaus adopts a philosophy of minimalism and accessibility (DAOHAUS, n.d.; Faqr-Rhazoui et al., 2021). Built upon the influential MolochDAO architecture, it provides a simple, straightforward, and relatively secure framework for communities to quickly form and operate. The core loop is lean: members pool capital into a shared treasury, vote on proposals to spend those funds, and, if they are ever dissatisfied with a governance outcome, retain the right to "rage quit" by immediately withdrawing their proportional share of the assets (Faqr-Rhazoui et al., 2021). This simplicity dramatically lowers the technical barriers to entry and deliberately avoids governance complexity, but it comes at the cost of limited functionality compared to more modular platforms. DAOhaus and the DAOs it enables exemplify a model of lean experimentation, prioritizing ease of use and rapid deployment over advanced or highly customized governance design.

Although most DAOs currently operate on the Ethereum network, the broader evolution of blockchain technology is rapidly expanding the possibilities for their design and application. The emergence of "Blockchain 2.0" applications, which extended beyond Bitcoin's initial function as a peer-to-peer currency, provided the programmable infrastructures necessary to host complex organizations (Cervone et al., 2020). Today, emerging blockchain ecosystems such as *Polkadot*, *Cosmos*, and *Solana* now compete to attract DAOs to their platforms, each offering different trade-offs in terms of transaction speed, cost, and cross-chain interoperability. This infrastructural diversification demonstrates that the manifestation of a DAO is deeply platform-dependent. The technical properties of the host blockchain, its throughput, transaction fees, and underlying consensus mechanism, directly shape the governance models and economic viability of the DAOs built upon it. For instance, the persistently high gas fees on the Ethereum mainnet have pushed many smaller or more transaction-intensive DAOs toward cheaper *layer-2 scaling solutions*⁶ like Optimism and Polygon. Thus, the underlying infrastructure is not a neutral backdrop but is rather a constitutive factor in DAO design and evolution.

4.5.3 Applications in Decentralized Finance

The most prominent and economically significant arena for the manifestation of DAOs is *Decentralized Finance (DeFi)*. Core DeFi protocols like *MakerDAO*, *Aave*, and *Uniswap* exemplify how DAOs can effectively govern complex financial infrastructures with treasuries valued in the billions of dollars. These DAOs are responsible for critical decisions, such as setting monetary policy for decentralized stablecoins (in the case of *MakerDAO*), adjusting the collateral requirements and interest rate parameters for lending pools (in the case of *Aave*), and controlling the fee structures for the world's largest decentralized exchanges (in the case of *Uniswap*) (Barbureau et al., 2022). These DeFi DAOs provide a powerful proof of concept that decentralized organizations can manage substantial and systemically important economic protocols without resorting to traditional centralized boards or executive teams. At the same time, they also serve as the most visible examples of the risks and pathologies discussed previously, including persistent voter apathy, the extreme concentration of voting power in the hands of a few "whales," and their ongoing vulnerability to sophisticated governance attacks.

4.5.3.1 *MakerDAO*

MakerDAO is one of the most established and systemically important decentralized autonomous organizations (DAOs) in the DeFi ecosystem. It governs the *Maker Protocol*, which issues the *DAI* stablecoin, an algorithmically maintained currency soft-pegged to the U.S. dollar and

⁶ Layer 2 solutions are secondary frameworks built atop a base blockchain (Layer 1) to improve performance and reduce transaction costs. They process transactions off the main chain and periodically record results back to it, maintaining security while enhancing efficiency. Common types include *rollups*, which bundle multiple transactions into a single on-chain record; *sidechains*, which operate as independent blockchains linked to the main network; and *state channels*, which allow participants to transact privately off-chain, recording only the final outcome on-chain.

backed by overcollateralized digital assets. MakerDAO's model represents an advanced experiment in decentralized monetary governance, demonstrating how financial stability can be maintained through transparent, community-driven decision-making rather than centralized control (Brennecke et al., 2022; MakerDAO, n.d.).

At the center of MakerDAO's governance lies the *MKR token*, which grants holders voting power over key protocol decisions. MKR holders act as both governors and risk bearers: if the system becomes undercollateralized, new MKR is minted and auctioned to cover losses, diluting existing holders; when the system operates profitably, MKR is bought back and burned, rewarding responsible governance. This structure directly links political authority with economic accountability, ensuring that those who steer the protocol share in both its risks and rewards.

The governance process operates through two interdependent mechanisms: *Governance Polls and Executive Votes*. Governance Polls are non-binding votes that gauge community sentiment on proposals, such as adding new collateral types, modifying stability fees, or adjusting liquidation ratios. Once a proposal gains sufficient support, it moves to an Executive Vote, a binding on-chain decision that enacts the change via smart contracts. This two-step process balances democratic deliberation with procedural discipline, ensuring that significant changes are both well-considered and technically sound.

To sustain complex operations, MakerDAO is organized into *Core Units*, autonomous, specialized teams responsible for domains such as risk management, protocol engineering, oracle infrastructure, and communications. Each Core Unit submits a charter and budget for MKR holder approval, and their performance is evaluated through transparent reporting. *Governance Facilitators* serve as intermediaries between Core Units and the community, maintaining procedural integrity and ensuring coordination across decentralized actors. This structure allows MakerDAO to combine open participation with professional management, effectively functioning as a "DAO bureaucracy" capable of executing long-term strategy.

Risk management is the cornerstone of MakerDAO's governance philosophy. Each collateral asset is subject to detailed evaluation by the Risk Core Unit, which assesses liquidity, volatility, and smart contract security before setting parameters such as the *debt ceiling*, *liquidation ratio*, and *stability fee*. The framework resembles a decentralized central bank's monetary policy, responsive, data-driven, and transparent. As co-founder Rune Christensen emphasized in his Devcon presentation, MakerDAO's approach constitutes a form of "scientific governance," where policy adjustments are based on continuous feedback and quantitative analysis rather than administrative decree.

Despite its sophistication, MakerDAO faces persistent challenges. Governance participation remains low, with only a fraction of MKR holders regularly voting, and the concentration of tokens among large holders ("whales") raises concerns about effective decentralization. The system's complexity also discourages less-technical participants, producing an implicit hierarchy of expertise. Moreover, the growing professionalization of Core Units, while improving operational efficiency, risks reintroducing the very centralization that DAOs were designed to avoid.

MakerDAO's resilience, however, has been proven through crises such as "*Black Thursday*" (March 2020), when market crashes led to undercollateralized DAI positions (Whiterabbit, 2020). Emergency votes and rapid policy adjustments stabilized the protocol, illustrating the DAO's adaptive capacity. Over time, MakerDAO has expanded its collateral base to include *real-world assets*, bridging decentralized governance with traditional financial systems and regulatory concerns.

In essence, MakerDAO exemplifies a *constitutional model of decentralized governance*, where power is distributed across code, economic incentives, and community deliberation. It demonstrates that decentralized systems can manage large-scale financial infrastructure, not through the absence of governance, but through the deliberate fusion of automation, transparency, and collective oversight.

4.5.3.2 Uniswap

Uniswap is one of the most influential decentralized autonomous organizations (DAOs) and a cornerstone of the Decentralized Finance (DeFi) ecosystem. Built on the Ethereum blockchain, it functions as an *automated market maker (AMM)* that enables users to swap ERC-20 tokens directly through liquidity pools, without intermediaries such as centralized exchanges or order books. Its governance structure, formalized through the *Uniswap DAO*, provides a compelling model of community-driven protocol management and demonstrates how decentralized decision-making can sustain a multibillion-dollar financial infrastructure (Uniswap Foundation, n.d.).

At its core, Uniswap operates on a simple yet elegant algorithmic principle: the *constant-product formula* ($x \times y = k$). This design ensures that liquidity pools remain balanced, whenever a user trades one token for another, the relative supply changes while maintaining a constant product. Liquidity providers (LPs) deposit token pairs into these pools and receive *liquidity tokens* representing their share. In return, they earn a proportional fraction of trading fees, which creates a self-sustaining incentive system for market liquidity. The protocol thus replaces the traditional market-making role of centralized entities with autonomous smart contracts, aligning user incentives with system stability.

The *Uniswap DAO* governs this ecosystem through the *UNI token*, which grants holders the right to propose, debate, and vote on protocol changes. Each UNI token corresponds to one vote, establishing a token-weighted voting model common in DeFi governance. Decisions subject to DAO control include adjusting fee structures, allocating treasury funds, upgrading core contracts, and managing incentive programs. The DAO treasury, containing over a billion dollars' worth of UNI tokens and protocol revenues, represents one of the largest decentralized treasuries in existence.

Governance in Uniswap follows a three-stage process. First, a *Temperature Check* is held off-chain on Snapshot to gauge community interest in a proposal. If it reaches a predefined quorum, it proceeds to an *On-Chain Consensus Check*, where voting power is formally tallied. Finally, successful proposals advance to an *Executive Vote*, which, upon approval, automatically

implements the change in smart contracts. This layered approach balances deliberation and decisiveness, ensuring that only well-supported, technically vetted proposals become binding. Governance discussions primarily occur on the *Uniswap Governance Forum*, enabling asynchronous participation and documentation of debate.

The Uniswap protocol has undergone several evolutionary upgrades that illustrate decentralized coordination at scale. *Uniswap v2 (2020)* introduced ERC-20/ERC-20 liquidity pairs, price oracles, and flash swaps, while *Uniswap v3 (2021)* revolutionized capital efficiency with *concentrated liquidity*, allowing LPs to allocate funds within specific price ranges. These innovations were debated, refined, and ratified through governance, demonstrating that decentralized communities can deliver complex technical progress without centralized leadership. The recent *Uniswap v4* initiative, introducing “hooks” for customizable liquidity and a unified pool architecture, continues this trajectory under DAO supervision.

Despite its successes, Uniswap governance faces challenges familiar to most DAOs. Participation rates remain low relative to total token distribution, with a small number of large holders, venture funds, early investors, and the Uniswap Foundation, exerting significant influence. Critics argue that this creates a *de facto plutocracy*, where financial power substitutes for democratic legitimacy. Moreover, the DAO’s global, pseudonymous composition complicates accountability and regulatory compliance, especially as Uniswap expands across multiple blockchain networks and integrates with real-world financial products.

Nonetheless, Uniswap remains a *benchmark for decentralized governance in DeFi*. It demonstrates how open protocols can coordinate global liquidity and evolve technically through transparent, rule-based collective processes. The Uniswap DAO merges algorithmic precision with community deliberation, showing that decentralized markets can achieve both operational efficiency and institutional continuity. Its continued evolution offers a model for how digital organizations can scale while preserving the founding ethos of open access, neutrality, and trustless exchange.

The underlying technology has also shown potential in the areas of remittances and financial inclusion. By reducing transaction fees and bypassing the costly network of traditional financial intermediaries, blockchain-based systems governed by DAOs could facilitate cheaper, faster, and more transparent cross-border payments (Campbell-Verduyn, 2017). Pilot projects in regions across Africa and Southeast Asia suggest that DAOs could become vehicles for local financial empowerment, though significant regulatory uncertainty and challenges related to usability and access remain formidable barriers to widespread adoption. Finally, the principles of DAO-like transparency and automation are being explored in the professional services sector. Major accounting firms have experimented with blockchain-based platforms to simplify auditing processes and reduce redundancy by creating a single, shared ledger for financial records (L. Liu et al., 2021). While not fully DAO-governed, these systems embody the core tenets of the model and raise important future questions about professional accountability and regulatory oversight if key financial infrastructures become community-governed.

While the DeFi ecosystem encompasses a vast number of DAOs operating at different layers of financial infrastructure, *MakerDAO* and *Uniswap* stand out as the most instructive and influential

examples. Together, they demonstrate how decentralized governance can effectively manage complex, high-stakes financial systems. These DAOs illustrate that blockchain-based collective decision-making, once considered experimental, can be executed successfully at scale, coordinating billions of dollars in assets without centralized oversight.

It is worth emphasizing that the *DeFi sector remains the most mature and successful testing ground* for DAO-based governance. While DAOs have found applications in numerous other fields, decentralized finance is where their structures have been most thoroughly implemented, stress-tested, and refined. Admittedly, the sector has also faced significant challenges, including high-profile incidents such as the *bZx exploit* and *The DAO hack*, which exposed the vulnerabilities of early smart contract design. Yet, these crises also served as crucibles for learning, prompting more resilient architectures, improved auditing standards, and stronger community-driven security practices. Despite these setbacks, DAOs continue to serve as the backbone of decentralized finance, governing protocols, managing treasuries, and setting monetary policy in a transparent and participatory manner.

This reality underscores a broader insight: *if DAOs can successfully coordinate and sustain an ecosystem as technically intricate and economically vital as DeFi*, they possess the structural potential to govern many other domains as well. Their ability to encode rules transparently, enforce them autonomously, and involve global stakeholders in governance processes makes them powerful organizational models for the digital age. As blockchain technology matures and as public understanding, trust, and regulatory clarity increase, it is reasonable to expect that DAOs will move steadily from the realm of finance into diverse fields, ranging from education and climate governance to social impact, creative industries, and urban management.

The following sections will explore these expanding frontiers, illustrating how DAOs are already being adapted across various sectors and how their underlying governance logic may redefine collective action in both digital and physical domains.

4.5.4 Philanthropy DAOs

DAOs have also begun to transform the landscape of philanthropy by introducing new ways to mobilize and distribute resources for the public good. These so-called philanthropy DAOs use blockchain-based infrastructures to ensure transparency, accountability, and community-driven decision-making in areas traditionally dominated by centralized intermediaries. Instead of relying on bureaucratic institutions or charitable trusts, these organizations leverage smart contracts and token-based voting to allocate funding more efficiently and equitably (World Economic Forum, 2022).

Prominent examples include *GitcoinDAO*, *EduDAO*, and *KlimaDAO*, each representing a distinctive approach to social impact within the decentralized ecosystem. *GitcoinDAO*⁷ provides funding for open-source software and digital public goods through a mechanism known as

⁷ see, Gitcoin DAO, <https://www.gitcoin.co/>

quadratic funding, which amplifies the influence of smaller individual contributions by matching them from a shared pool. This method ensures that community preferences, rather than wealth concentration, determine how resources are distributed, thereby democratizing public goods funding. *EduDAO*,⁸ on the other hand, bridges academic institutions with blockchain communities, providing grants that support student-led innovation, research, and education projects. By removing institutional intermediaries, EduDAO directly connects academic creativity with decentralized financing, fostering a new culture of academic autonomy and experimentation. *KlimaDAO*⁹ advances environmental objectives by tokenizing carbon credits, allowing participants to purchase, retire, or trade these tokens as part of a decentralized carbon market. Through this structure, KlimaDAO aligns blockchain incentives with global sustainability targets, illustrating how decentralized governance can support environmental, social, and governance (ESG) principles on a global scale. Together, these organizations exemplify a growing movement in which DAOs serve as transparent, globally coordinated vehicles for philanthropic activity, shifting the paradigm of charity from trust-based to verifiability-based systems of impact.

4.5.5 Societal Impact DAOs

Beyond philanthropy, DAOs are increasingly emerging as decentralized infrastructures for addressing complex global challenges such as humanitarian crises, climate change, and public goods coordination. These impact DAOs operate as agile, trust-minimized institutions capable of responding rapidly to emergencies and facilitating global cooperation without the overhead of traditional governance systems (World Economic Forum, 2022).

A notable example is *UkraineDAO*,¹⁰ which was established during the early days of the 2022 Russian invasion of Ukraine to raise humanitarian aid. The DAO successfully collected over six million dollars in cryptocurrency donations within days, distributing the funds directly to relief organizations in a transparent and traceable manner. This case demonstrated the potential of DAOs as rapid-response funding mechanisms that bypass conventional bureaucratic and geopolitical bottlenecks. Similarly, environmental DAOs such as ReFi DAO¹¹ and Toucan DAO¹² focus on sustainability and carbon market coordination by creating decentralized registries and trading systems for verified carbon credits. By doing so, they democratize access to climate finance and increase accountability in environmental reporting.

At the same time, *MolochDAO*,¹³ one of the earliest and most influential DAOs, pioneered decentralized funding models for open-source development within the Ethereum ecosystem. Its structure inspired numerous successors, including *MetaCartel DAO*,¹⁴ which finances early-stage

⁸ see, EduDAO, <https://edudao.io/>

⁹ see, KlimaDAO, <https://www.klimadao.finance/>

¹⁰ see, UkraineDAO, <https://ukraine-dao.notion.site/Ukraine-DAO-3a0e63c6190b4796890dec5c72a94872>

¹¹ see, ReFi DAO, <https://www.refidao.com/>

¹² see, Toucan DAO, <https://toucan.earth/>

¹³ see, MolochDAO, <https://molochdao.com/>

¹⁴ see, MetaCartel DAO, <https://www.metacartel.org/>

decentralized applications and ecosystem infrastructure. These DAOs collectively demonstrate the growing role of decentralized governance in addressing public needs, from climate resilience to digital infrastructure. By operating on-chain with open treasuries and traceable transactions, they embody a form of institutional transparency that strengthens legitimacy and public trust in collective action.

4.5.6 Community, Labor, and Network Coordination

DAOs are also reshaping the organization of digital labor, professional collaboration, and creative communities. Instead of relying on hierarchical corporate structures, these organizations coordinate contributions through smart contracts, aligning incentives with reputation and performance rather than formal employment relationships. This emerging *post-corporate* model allows individuals to participate in multiple organizations simultaneously, contributing expertise across projects and being compensated directly in tokens or stablecoins (World Economic Forum, 2022).

Projects such as *Raid Guild*¹⁵ and *dOrg DAO*¹⁶ exemplify this paradigm by coordinating teams of developers, designers, and strategists through decentralized work agreements. Tasks are managed, verified, and compensated automatically through on-chain contracts, reducing administrative friction and ensuring payment transparency. Similarly, *Friends with Benefits (FWB)*¹⁷ and *Black Flag DAO*¹⁸ blur the line between social networks and professional communities. They function as digital cooperatives where members contribute content, events, and research, earning governance tokens that grant both ownership and influence in shaping the organization's direction. This fusion of community, identity, and labor coordination signals a broader evolution toward participatory digital economies in which work is modular, reputation-based, and globally distributed.

4.5.7 Governance Innovation and Civic Applications

Finally, DAOs are increasingly recognized as *laboratories of governance*, where new models of collective decision-making and digital democracy are being tested. Through mechanisms like *quadratic voting*, *delegated decision-making*, and *on-chain constitutional frameworks*, DAOs experiment with systems that could influence how future civic and institutional governance operates. The *CityDAO* project in Wyoming provides a compelling real-world example: it uses blockchain to enable tokenized property rights and participatory land management, exploring how decentralized coordination might enhance municipal governance.

¹⁵see, Raid Guild DAO, <https://www.raidguild.org/>

¹⁶see, dOrg DAO, <https://www.dorg.tech/>

¹⁷see, Friends with Benefits DAO, <https://www.fwb.help>

¹⁸see, Black Flag DAO, <https://blackflagdao.notion.site/>

The experiments could shape the next generation of *participatory governance systems*, from citizen-driven budgeting to transparent policy enforcement (World Economic Forum, 2023). By embedding procedural fairness and accountability directly in code, DAOs hold the potential to augment or even partially replace traditional bureaucratic processes, offering scalable, transnational models for democratic coordination.

4.5.8 Manifestations of Crisis and Confrontation

No discussion of the practical manifestation of DAOs is complete without acknowledging the crises that have defined their evolution and their ongoing confrontation with state power. Controversial cases such as Ooki DAO and Tornado Cash illustrate how these novel entities can directly challenge and sometimes actively resist regulatory enforcement. The core of the conflict lies in the difficulty courts and regulators face in attributing legal liability when decision-making authority is distributed across a pseudonymous, often global, community of token holders (De Filippi et al., 2024). This has led to the concept of "alegality," which describes how certain technologies operate in a legal gray zone, outside of or in direct opposition to existing legal frameworks. The case of Tornado Cash, a privacy-enhancing protocol governed by a DAO, is particularly instructive. In 2022, the U.S. Treasury Department sanctioned the protocol, alleging its use for money laundering (U.S. Department of Treasury, 2022). This action, which targeted the protocol's code itself and led to the arrest of one of its developers, demonstrated that the supposed autonomy of a DAO does not grant it immunity from state power. The case highlights that the manifestation of DAOs is not a purely technical or economic phenomenon but is deeply entangled with legal recognition, state authority, and geopolitical considerations.

Finally, as examined previously, the 2016 hack of The DAO remains the canonical failure that continues to haunt the ecosystem. Launched as a decentralized venture fund on Ethereum, it raised over \$150 million in what was then the largest crowdfunding campaign in history. Shortly after, a vulnerability in its smart contract was exploited, allowing an attacker to drain a significant portion of the funds and triggering one of the most significant crises in blockchain history. The event forced the Ethereum community into a contentious and divisive decision: uphold the absolutist principle of "code is law" or intervene with a hard fork to restore the stolen funds. The community chose intervention, creating a permanent split in the blockchain, resulting in Ethereum (ETH) and Ethereum Classic (ETC). This formative crisis crystallized the tension between rigid algorithmic authority and the necessity of human judgment when faced with catastrophic failure. Other notable incidents have since followed, such as the 2020 bZx DAO exploit, where flash loan manipulation enabled attackers to momentarily control governance and siphon funds, and the 2022 Wormhole bridge hack, which led to a loss of over \$300 million due to vulnerabilities in cross-chain protocols (Bannister, 2021; Chainanalysis, 2022). These cases reinforce the persistent vulnerabilities in DAO governance and smart contract security, highlighting the inescapable complexities of decentralized governance and the ongoing need for careful oversight and intervention. The DAO hack remains the most powerful cautionary tale frequently cited in discussions of immutability, governance limits, and blockchain resilience.

Beyond these specific crises, the broader landscape of DAO manifestations is marked by a distinct sense of ambiguity and provisionality. Many of the applications that generate excitement exist more as aspirations or early-stage prototypes than as fully established and robust practices (Campbell-Verduyn, 2017). DAOs often operate as functional experiments, sufficiently developed to test novel concepts but not yet mature or resilient enough to fully replace the established institutions they seek to disrupt. This emergent character means that the field is a site of ongoing negotiation between competing ideals: the push for radical decentralization versus the pragmatic need for efficiency; the commitment to absolute openness versus the fundamental requirements of privacy; and the desire for permissionless innovation versus the growing pressures of legal and regulatory compliance. Many DAO initiatives fail quietly, while others pivot into hybrid forms that blend the novel features of the DAO model with the stability and legal recognition of traditional organizational structures.

This process of manifestation is also expanding the very objects of governance beyond the organization itself. In this new paradigm, governance extends to the underlying protocols that support entire ecosystems, the on-chain data that represents collective history and assets, and the off-chain communities that provide social legitimacy and direction (Y. Liu et al., 2023). Disputes over intellectual property, data access, or protocol upgrades in DAOs highlight how longstanding problems in fields like Data Asset Management (DAM) and System Architecture Design (SAD) are being instantiated in new digital and decentralized forms (Ziolkowski et al., 2020a). The manifestation of DAOs is therefore not only about the formation of new organizations but also about the fundamental redefinition of what constitutes a governable object in a digital economy. This perspective on their real-world application, with its mix of promise and fragility, complements the preceding economic analysis and sets the stage for a final, holistic conclusion on the state and future of this transformative organizational model.

4.6 Conclusion: DAOs as new forms of governance

The emergence of Decentralized Autonomous Organizations represents a genuine paradigm shift in organizational theory and a powerful practical experiment in the future of human coordination. Built on the architectural foundations of blockchain technology, DAOs challenge the centuries-old hierarchical structures that have long dominated our economic and social landscapes. By embedding rules in transparent, automated, and immutable code, they advance a compelling vision of organizations that are more equitable, efficient, and directly controlled by their stakeholders. Throughout this chapter, we have traversed the foundational principles, governance mechanisms, economic logics, and practical manifestations of this novel organizational form. The journey reveals a landscape rich with innovation but also fraught with deep and persistent tensions that temper the most utopian claims of its proponents.

The central and recurring theme in the analysis of DAOs is the profound and often irreconcilable conflict between their decentralized aspirations and the practical realities of their implementation. The ideal of a truly leaderless, trustless organization that is governed purely by algorithmic consensus remains elusive. In its place, we find a consistent re-emergence of centralization in new forms: voting power concentrates in the hands of wealthy "whales," creating digital timocracies;

technical complexity grants disproportionate influence to a small cadre of core developers, creating informal hierarchies of knowledge; and the need for legal and strategic agility often leads to the formation of off-chain foundations and committees that act as de facto leadership bodies. The promise of a "trustless" system based on verifiable code is similarly complicated by the persistent and indispensable role of human trust. DAOs remain deeply dependent on trust in the developers who write their code, trust in the off-chain social consensus that legitimizes critical decisions, and trust in the oracles that feed them vital real-world information.

Furthermore, the core architectural strengths of the DAO model, automation and immutability, are the source of its most significant weaknesses. The efficiency and predictability gained through smart contract automation are achieved at the cost of adaptability. The rigid, deterministic nature of code struggles to accommodate the ambiguity, nuance, and unforeseen "black swan" events that define the real world. As the hacks in the field, the most critical moments in an organization's life often reveal the inescapable need for adaptive, context-aware human judgment that code alone cannot provide. Similarly, the ideal of radical transparency, which promises unprecedented accountability, creates a direct conflict with the fundamental rights to individual privacy and the need for strategic discretion in competitive environments.

Ultimately, the story of the DAO is a story of the gap between a powerful, revolutionary rhetoric and the messy, complex, and often contradictory reality of its execution. They are not, as of yet, a perfected replacement for traditional firms, but rather a vast, real-time laboratory for institutional innovation. Their greatest contribution may not be the answers they have provided, but the critical questions they are forcing us to ask about the very nature of trust, power, governance, and value in the 21st century.

The future evolution and long-term success of this organizational form will likely depend not on a rigid adherence to technological purity, but on the ability of their communities to design more sophisticated and resilient hybrid models. These future systems must find ways to effectively blend the accountability and automation of on-chain mechanisms with the flexibility and nuanced deliberation of off-chain human governance. The critical unresolved questions that will define the next phase of their development remain formidable. How can DAOs design more equitable and inclusive governance systems that can meaningfully resist the powerful gravitational pull of plutocracy? How can they navigate the deep-seated legal and regulatory ambiguities that currently limit their ability to interact with and reform the traditional economy? And how can they strike a sustainable balance between the rigid predictability of code and the adaptive wisdom of the collective? The answers to these questions are not yet clear, but the ongoing pursuit of them marks the DAO as one of the most significant and compelling organizational experiments of our time.

5 Chapter 4: Blockchain Technology and Law from the Perspective of Decentralized Autonomous Organizations and the Corporate Law

5.1 Introduction and Research Context

As established in the preceding chapters, the path to mainstream adoption for blockchain technology is fraught with challenges, the most significant of which is the lack of clear legal recognition and regulatory coverage. Whereas the previous chapter examined Decentralized Autonomous Organizations (DAOs) as novel experiments in private governance, this chapter confronts the critical legal and institutional consequences of that experiment. While the technology emerged with the ideological motivation of replacing trusted intermediaries with self-enforcing smart contracts, its practical application has demonstrated that this ideal is far from reality. Blockchain applications remain subject to existing laws and must adapt to these frameworks to survive and scale.

At the core of these applications are DAOs, internet-native entities built on blockchain technology that operate according to rules encoded in smart contracts rather than legal charters. This model has fueled rapid innovation, particularly in Decentralized Finance (DeFi), with collective treasuries now valued at \$17.8 billion and a global participant base of 11.8 million token holders as of May 2025 (DeepDao, n.d.). This growing scale renders the need for their legal recognition urgent. Yet, this explosive growth has occurred in a legal vacuum. In the absence of clear legal recognition, DAOs face the imposition of ill-fitting and often severe legal defaults. In most jurisdictions, these entities have been treated as *general partnerships* by default, subjecting all members to unlimited liability, a strict requirement that clashes with the pseudonymous and fluid nature of DAO participation.

This chapter therefore investigates the profound tension that arises when decentralized organizations meet legal systems designed for centralized entities. It confronts this issue by systematically evaluating the suitability of emerging corporate law-based solutions, such as new DAO-specific statutes. To do so, it undertakes a *comparative analysis*, contrasting the foundational principles of corporate law with the unique attributes of DAOs to highlight the specific differences that challenge legal adaptation. This analysis serves as a critical case study for the broader challenge of aligning blockchain technology with existing legal frameworks, providing a comprehensive overview of current regulatory responses and proposing a forward-looking regulatory blueprint.

5.1.1 Research Statement and Questions

The principal aim of this chapter is to investigate the critical tension between blockchain technology and law, focusing on Decentralized Autonomous Organizations (DAOs) as the most

advanced application of blockchain for organizational governance. It argues that the current legal treatment of DAOs, particularly their default classification as general partnerships, *is conceptually unsound and practically unsustainable*, creating a major obstacle to their future development. The chapter explores how the novel features of DAOs, such as decentralization and immutability, make their adaptation into existing legal frameworks uniquely challenging.

To address this, the chapter confronts a central theoretical question: How can a decentralized organizational form be understood and regulated within legal systems designed for centralized entities? This inquiry requires a systematic evaluation of the suitability of corporate law-based solutions, which pioneering jurisdictions are currently attempting to apply. By contrasting the foundational principles of corporate law with the unique attributes of DAOs, this chapter aims to develop a normative framework capable of aligning these novel organizational technologies with legal requirements.

Accordingly, this chapter is guided by the following research questions:

1. How do the foundational principles of corporate law (e.g., legal personality, limited liability, delegated management) conflict with the unique technological and organizational attributes of DAOs?
2. What are the legal and practical consequences of DAOs being treated as general partnerships by default, particularly regarding member liability?
3. How effective are current legislative innovations, such as the DAO LLC statutes in the United States, and "legal wrappers" in resolving the core challenges of liability and legal personality?
4. What does a comparative analysis of regulatory responses in the United States and the European Union reveal about the fragmented path toward legal certainty for DAOs?

By addressing these questions, the chapter positions DAOs as a critical case study for the broader challenge of integrating blockchain technology into established legal systems.

5.1.2 Methodological Framework

This chapter employs a *qualitative, interpretive research paradigm* to examine the complex relationship between law, governance, and technology. The core research question revolves around how a decentralized organizational form (DAO) can be understood and regulated within legal systems designed for centralized entities. This inquiry is not about quantitative metrics but about the *normative conflicts and institutional obstacles* that define the current legal landscape for DAOs. An interpretive approach is essential for a deep, contextualized understanding of this phenomenon, recognizing that the legal status of DAOs is shaped by the legal and regulatory environments they encounter.

5.1.2.1 Research Design and Approach

The chapter is designed as a *comprehensive, multi-disciplinary, literature-based study* that uses a method of *thematic synthesis*. This approach is well-suited for a rapidly evolving field where

knowledge is spread across disparate texts. The chapter aims to construct a coherent argument about the legal challenges facing DAOs by synthesizing existing knowledge from diverse fields.

5.1.2.2 Data Collection

The primary data for this chapter consists of a curated body of textual sources, selected to provide a holistic view of the research problem. These sources include:

- **Doctrinal Legal and Jurisprudential Scholarship:** This includes law review articles and academic treatises on corporate law, partnership law, and the emerging field of "blockchain law." This literature forms the basis for understanding the foundational principles of corporate governance and the legal challenges posed by DAOs.
- **Technical and Computer Science Literature:** Foundational technical papers and explanatory texts were reviewed to ensure an accurate understanding of blockchain's core properties, such as smart contracts and consensus mechanisms for a better illustration of their legal implications.
- **Grey Literature and Empirical Case Studies:** This includes reports from regulatory bodies (like the SEC and CFTC), white papers from specific DAO projects, policy analyses from international organizations, and research from think tanks. This literature provides the empirical grounding for the analysis of regulatory actions and real-world legal challenges.

5.1.2.3 Method of Analysis

The analysis of the collected literature was conducted using a thematic synthesis approach. This involved a three-stage process:

1. **Free Line-by-Line Coding:** A thorough reading of all selected texts was undertaken to identify key concepts, arguments, and legal precedents.
2. **Organization into Descriptive Themes:** The initial codes were then grouped into a hierarchical structure of related "descriptive themes." These represent recurring issues identified across the literature, such as the problem of legal personality, the risk of unlimited liability, and the challenges of applying securities law.
3. **Generation of Analytical Themes:** The final stage involved moving beyond description to interpretation. The descriptive themes were synthesized to generate higher-order "analytical themes" that form the core argument of the chapter, building a central narrative about the clash between decentralized organizations and traditional legal frameworks.

5.1.3 Contribution

Methodologically, this chapter bridges the gap between *socio-technical systems analysis* and *doctrinal legal theory*. It contributes to the growing field of *blockchain law* by moving beyond

high-level policy debates to conduct a systematic, comparative analysis between the essential features of corporate law and the unique architecture of DAOs. By dissecting the specific points of friction, legal personality, liability, and fiduciary duties, this chapter provides a granular framework for legal scholars and policymakers. Its primary contribution is the development of a coherent regulatory blueprint that addresses the "governance paradox" of DAOs, offering a path to reconcile their decentralized ethos with the fundamental requirements of legal accountability.

5.1.4 Literature Review

The legal and organizational challenges of Decentralized Autonomous Organizations (DAOs) emerge within a rapidly developing interdisciplinary field. Early literature often celebrated decentralized governance as a technological alternative to the state and the corporation, whereas more recent work emphasizes the need to reconcile these innovations with long-established legal institutions. Across these phases, scholarship increasingly reveals that DAOs disrupt foundational legal assumptions regarding personhood, liability, ownership, and regulatory accountability, thereby challenging the conceptual boundaries of corporate law and exposing critical gaps in existing frameworks (Allen, 2020; Kaal, 2019; Nunes Teixeira, 2023).

A first and enduring point of reference is *corporate law theory*, which provides the dominant blueprint for organizing economic activity at scale. Kraakman et al. (2017) identify five essential attributes of the corporate form, legal personality, limited liability, transferable shares, delegated management, and investor ownership, that jointly enable capital aggregation, risk diversification, and efficient governance. Scholars have long demonstrated the economic rationality of these features: limited liability incentivizes investment by capping downside risk (Easterbrook & Fischel, 1985), transferable shares facilitate liquidity (Manne, 1967), and delegated management addresses the coordination challenges arising from dispersed ownership (Armour et al., 2017). This literature establishes the legal and institutional “baseline model” against which DAO architecture and governance innovations are evaluated.

Working in tension with this legal tradition is a second body of literature grounded in *blockchain ideology and socio-technical governance*. The cypherpunk and crypto-anarchist foundations of blockchain popularized the “code is law” thesis, arguing that trust and legal order could be enforced through cryptography rather than the state (Lessig, 2009; De Filippi & Wright, 2018). Proponents envisioned smart contracts as replacements for corporate charters and managerial oversight, enabling decentralized, automated, and censorship-resistant rule enforcement (Werbach, 2018; Mehar et al., 2019). However, critical legal scholarship rejects this technological reductionism, stressing that law is an irreducible expression of sovereign authority and public policy (Borgogno & Martino, 2024; Østbye, 2024). When blockchain interactions generate real-world externalities, courts apply traditional legal doctrines rather than deferring to on-chain technical rules (Hacker, 2019). This literature makes clear that the legal system does not, and cannot, treat code as a substitute for legally recognized entity status or liability allocation.

Bridging these theoretical poles, a growing body of *applied and doctrinal legal scholarship* examines how existing law treats DAOs in practice. The dominant finding is a

dangerous legal default: in most jurisdictions, absent formal incorporation, DAOs are classified as *general partnerships* or unincorporated associations, thereby exposing governance participants to joint and several personal liability (Kaal, 2019; Weinsten & Loftchie, 2022; Zetsche et al., 2018). This risk is no longer hypothetical. Landmark U.S. cases such as *CFTC v. Ooki DAO* and *Sarcuni v. bZx DAO* have held token-holders personally liable for the organization's regulatory violations and financial losses (Commodity Futures Trading Commission, 2023; Drylewski, 2023; Pascoe, 2023). These decisions demonstrate that decentralization does not insulate participants from enforcement. This line of literature also exposes the “*interface problem*”, DAOs' inability, without legal personality, to hold property, enter into enforceable contracts, or appear in court (Boss, 2023; Sims, 2019).

An additional dimension of legal scholarship focuses on *regulatory experimentation and legislative innovation*. Several U.S. states, including Wyoming, Utah, and Vermont, have introduced DAO-specific legal forms, such as the *DAO LLC*, in an effort to extend liability protection while accommodating decentralized governance (Beckett, 2023; Brummer & Seira, 2022). A parallel, practice-based approach deploys “*legal wrappers*,” such as foundations or conventional LLCs, to provide DAOs with a juridical interface to the off-chain world (de Oliveira & Rolo, 2023; World Economic Forum, 2022). Yet scholars emphasize that these solutions remain fragmented, often reintroducing centralized points of control and failing to achieve robust cross-border recognition (Garcia Rolo, 2019; Biyan Mienert, 2024). This literature repeatedly underscores a core tension: DAOs are borderless digital networks operating under territorially bound legal regimes.

Finally, an important emergent strand confronts the *governance and enforcement paradox* at the heart of DAOs. While decentralization aims to avoid corporate hierarchy, functional governance often recentralizes authority through core developers, multisignature key-holders, or major token-holders (Hassan & De Filippi, 2021; DuPont, 2017; Sharma et al., 2024). Empirical analyses of governance failures, including flash-loan voting attacks, highlight that algorithmic automation introduces novel risk vectors rather than eliminating managerial discretion (Lehar & Parlour, 2022; Reijers et al., 2021). These studies consistently conclude that DAOs do not escape the need for regulatory oversight, fiduciary obligations, or actor-level accountability, rather, they transform where those obligations must be situated and how they can be enforced.

Taken together, the literature reveals an ongoing conceptual and institutional struggle. Corporate law scholarship provides a stable architecture for rights and responsibilities, while blockchain governance theory challenges its anthropocentric and territorial assumptions. Applied legal research demonstrates that courts will enforce liability and regulatory compliance even when control is dispersed through code. Legislative innovations remain promising but incomplete. This chapter builds on these scholarly foundations by conducting a systematic comparison between the essential features of corporate law and the unique structure of DAOs, in order to articulate a coherent regulatory model that can bridge the gap between decentralized governance and legal accountability.

5.2 Setting the Stage: Current State-of-Art of DAOs

Blockchain governance represents a paradigm shift in organizational theory and practice, emerging as internet-native entities constructed upon the architectural foundations of blockchain technology. Decentralized Autonomous Organizations are the most illustrative example as an embodiment of the blockchain's potential in governance domain. These novel structures operate according to foundational rules and operational logic that are not inscribed in legal charters but are encoded directly into smart contracts. These self-executing scripts ensure that a DAO's processes are transparent, immutable, and largely autonomous, with the locus of decision-making power typically distributed among a global community of token-holding members. This model stands in stark contrast to the hierarchical and permissioned structures of traditional organizations, enabling a form of governance where members collectively manage treasuries, vote on strategic proposals, and finance a diverse array of projects, particularly within the burgeoning field of Decentralized Finance (DeFi) and collaborative investment. The aspiration of this model is to achieve a state of community-driven governance characterized by enhanced resilience and alignment of interests.

The proliferation and economic impact of DAOs are no longer matters of niche speculation. As of May 2025, their collective treasuries were valued at an astonishing \$17.8 billion, with a participant base of 11.8 million token holders distributed across the globe, underscoring their rapid ascent as significant economic actors (DeepDao, n.d.). However, this explosive growth has occurred within a critical legal and regulatory vacuum. The absence of bespoke legal frameworks is becoming increasingly untenable as the ecosystem contends with a rising tide of security breaches, hacks, and fraudulent activities, which in turn intensifies the pressure on legislatures and regulatory bodies to provide specific and effective guidelines. In the absence of such tailored legal structures, DAOs frequently default to the legal classification of a general partnership in many common law jurisdictions.

This default designation is catastrophically ill-suited for these organizations. It subjects their members, who are often pseudonymous, geographically dispersed, and participating on a fluid basis, to the draconian penalty of unlimited personal liability for the entirety of the organization's debts and legal obligations. While some scholars and practitioners have looked to existing corporate law as a potentially more appropriate framework, a fundamental tension persists. DAOs differ substantially not only from general partnerships but also from the very corporations whose legal forms they might otherwise adopt, making the wholesale application of established corporate law a challenging and often distorting exercise. The promise of blockchain technology to enhance corporate governance by eliminating certain forms of intermediation presents a compelling opportunity, yet this potential is constrained by the profound legal uncertainties that currently prevail (Akgiray, 2019). The distance between the ultimate owners of capital and the corporate users of that capital has grown due to a complex web of intermediaries, a problem that decentralized technology aims to solve.

This chapter confronts this nuanced and critical discussion directly. It will first illuminate the structural and philosophical novelty of DAOs by systematically contrasting them with traditional corporations, thereby fostering a deeper understanding of their unique attributes and operational logics. This comparative analysis will serve a dual purpose: to highlight the innovations of the DAO model and to critically evaluate the suitability of applying established corporate law

principles to it. Following this foundational examination, the chapter will present a comprehensive overview of the current regulatory responses to DAOs in two of the world's most influential legal spheres: the United States and the European Union. Drawing upon the insights gained from the analysis of DAO characteristics and the current regulatory environment, the study will then dissect the key legal and regulatory hurdles that impede the maturation and mainstream adoption of these organizations. Finally, the chapter will conclude by proposing a series of forward-looking recommendations designed to forge a path toward greater legal clarity and certainty for DAOs, enabling them to flourish responsibly within the global economy.

5.3 DAOs and Traditional Corporations

While the details of corporate law differ across jurisdictions, a relatively stable set of foundational legal principles has defined the architecture of the modern business corporation across the globe. Regardless of whether one examines Anglo-American common law systems, continental European civil law traditions, or hybrid jurisdictions, the corporate form has converged around certain essential features that enable it to function as the dominant vehicle for organizing large-scale economic activity. To establish a coherent basis for comparison, this chapter adopts the seminal analytical framework proposed by Kraakman et al. (2017), which identifies five defining attributes of the corporate form: *legal personality*, *limited liability*, *transferable shares*, *delegated management under a board structure*, and *investor ownership* (Kraakman et al., 2017).

These five characteristics together constitute more than a checklist of institutional traits; they form an interdependent system that allows corporations to mobilize and coordinate human and financial capital at scale. Legal personality permits the corporation to exist as a distinct juridical entity, capable of owning property, entering contracts, and being held accountable independently of its members. Limited liability shields shareholders from the corporation's debts, thereby encouraging investment and risk-taking. Transferable shares provide liquidity and enable dynamic reallocation of ownership interests, facilitating efficient capital markets. Delegated management under a board structure introduces a mechanism for professionalized governance, separating ownership from control while maintaining accountability through fiduciary duties. Finally, investor ownership aligns the residual claimants with the goal of profit maximization, giving coherence to corporate decision-making.

This doctrinal synthesis offers a powerful conceptual lens through which to examine *Decentralized Autonomous Organizations (DAOs)*. By mapping these five corporate features onto the emerging architecture of DAOs, the chapter exposes not only areas of structural resemblance, such as collective ownership and governance delegation, but also points of deep divergence. DAOs challenge the anthropocentric assumptions of corporate law by replacing human intermediaries with algorithmic coordination, blurring the boundaries of ownership, agency, and accountability. A systematic comparison along these five dimensions thus becomes indispensable for revealing the philosophical tensions, operational uncertainties, and legal design challenges that DAOs face as they seek legitimacy and integration within existing economic and regulatory systems.

5.4 Legal Personality: The Foundational Challenge for DAOs

At the heart of the modern global economy lies a legal artifice of profound consequence: the principle of legal personality. It is, perhaps, the single most pivotal innovation in the history of commercial law, a conceptual contrivance that permits a collective human enterprise to transcend the inherent limitations of its individual members. This principle embodies the profound conceptual leap of recognizing a business organization as an entity that is legally separate and distinct from the people who own, manage, or work for it. In the eyes of the law, the corporation becomes an "artificial person," a legal fiction that, despite its abstract nature, is endowed with a suite of concrete rights and responsibilities that make large-scale, long-term commerce possible (Kraakman et al., 2017). This status is not an inherent quality that an organization possesses by virtue of its existence; rather, it is an "institutional" concept, a privilege conferred by a sovereign state through a deliberate legal act, typically involving registration with a governmental agency or a direct charter from the legislature (Florian Möslin & Daniel Ostrovski, 2024).

The historical impetus for this legal invention was born of necessity. As economies evolved beyond local artisanship and regional trade, ambitious ventures such as transoceanic voyages, the construction of canals, and the laying of vast railway networks required capital far exceeding the wealth of any single individual or small consortium of partners. These monumental undertakings also involved immense risks and time horizons that often spanned generations, rendering the traditional partnership model wholly inadequate. In a partnership, the organization's legal identity was fused with that of its owners; consequently, if a partner died, became insolvent, or simply chose to exit, the entire legal structure of the enterprise could dissolve, creating instability and chaos for investors, creditors, and employees alike.

Corporate legal personality provided an elegant solution to these problems. By creating a distinct and durable entity, it granted the enterprise the gift of perpetual succession, the capacity to exist indefinitely, independent of the lives, fortunes, or whims of its founders and subsequent shareholders (Schwartz, 2011). This inherent stability was the essential precondition for attracting the vast sums of public capital required to fuel the Industrial Revolution and the subsequent waves of economic expansion. The practical capacities bestowed by this artificial personhood are the engine of its economic power. A corporation, in its own name, can own the full spectrum of assets, from real property and factories to intellectual property such as patents and copyrights. It can enter into legally binding contracts with suppliers, customers, and employees; it can incur its own debts and liabilities; and, critically, it can sue or be sued in its own name in a court of law (Charlton et al., 2023; Kraakman et al., 2017).

Furthermore, the principle of legal personality is the indispensable prerequisite for a critical mechanism known as entity shielding. This legal doctrine segregates the assets owned by the corporation from the personal assets of its shareholders, creating a protective barrier that is essential for the firm's stability and longevity. This means that the personal creditors of a shareholder cannot seize corporate property, such as its factories, bank accounts, or intellectual property, to satisfy a private debt owed by that shareholder. This ensures that the operational assets of the business remain intact, dedicated solely to the firm's productive purpose, and insulated from the personal financial vicissitudes of its owners (Florian Möslin & Daniel Ostrovski, 2024). This partitioning of assets is what solidifies the corporation's role as a predictable and reliable

counterparty in the marketplace, and it serves as the necessary foundation for the corporation's most famous and economically vital feature: limited liability (Millon, 1990).

However, an artificial person, being "invisible, intangible, and existing only in contemplation of law," is fundamentally inert; it cannot think, speak, or act of its own volition (Florian Möslin & Daniel Ostrovski, 2024). The law bridges this conceptual gap between an abstract entity and its capacity for real-world action through the sophisticated doctrine of legal agency. The corporation, acting as a legal principal, empowers designated human agents, its board of directors and executive officers, to act on its behalf (J. G. Allen, 2020; Florian Möslin & Daniel Ostrovski, 2024). It is through the decisions, deliberations, and signatures of these legally recognized individuals that the corporation enters into contracts, manages its complex operations, and engages with the wider world. These human "organs" serve to animate the corporate form, transforming it from a passive legal construct into an active and dynamic economic subject (J. G. Allen, 2020). This framework of agency is not merely a matter of practical convenience; it is a legally refined system for delegating authority, managing immense complexity, and establishing clear channels of accountability for the entity's actions (Borgogno & Martino, 2024; Hacker, 2019). In essence, the law of agency provides the vital nervous system that allows the artificial person of the corporation to function effectively.

5.4.1 DAOs and the Absence of Personhood

It is into this deeply entrenched, state-centric legal tradition that the Decentralized Autonomous Organization emerges as a radical and disruptive force. A DAO, in its purest theoretical form, is an organization that exists not as a file in a government registry but as a software protocol operating on a blockchain network. Its governing rules are not written in a corporate charter but are encoded in smart contracts, self-executing scripts that automate its operations and governance processes with mathematical precision. Decision-making authority is not vested in a board of directors appointed by shareholders but is distributed among a potentially vast, pseudonymous, and globally dispersed community of token holders who collectively manage the entity's actions and resources.

This unique architecture presents a fundamental challenge to the established legal paradigm of personhood. In its native, purely code-based form, a DAO lacks any independent legal status. It is not automatically recognized as a distinct entity by legal systems that have spent centuries constructing frameworks predicated on the principles of state registration and formal, sovereign recognition (De Filippi & Wright, 2018). Consequently, for a DAO to acquire the benefits of legal personhood, it requires explicit recognition from a legal jurisdiction. However, the idiosyncratic nature of DAOs, particularly their decentralized governance structures and reliance on autonomous code, presents a significant challenge to traditional legal frameworks, making this recognition process neither simple nor straightforward. Therefore, a native DAO, existing as a mere software construct, is legally incapable of performing the most basic functions of a legal person: it cannot hold title to physical property, sign an enforceable off-chain contract with a service provider, or appear as a plaintiff or defendant in litigation.

5.4.2 The Default Status: General Partnership and Unlimited Liability

This profound disconnect between the on-chain reality of the DAO and the requirements of the off-chain legal world is not accidental but deeply philosophical. The genesis of DAOs is rooted in a cypherpunk ethos of "code is law." This philosophy posits that the formal legal system, with its reliance on trusted human intermediaries such as lawyers, judges, and regulators, is inherently inefficient, costly, and susceptible to error, bias, or corruption. The proposed alternative was a system of "trustless" governance, where an organization's operational logic is immutably and transparently encoded in a smart contract, with its rules automatically enforced by a decentralized network. In this vision, there is no need for traditional legal enforcement mechanisms because the code itself serves as the final and incorruptible arbiter of rules and outcomes (J. G. Allen, 2020; Nunes Teixeira, 2023). The promise was one of radical disintermediation and legal self-sufficiency, where the elegant certainties of software and cryptography would replace the fallible and often costly interventions of trusted human third parties (Borgogno & Martino, 2024).

However, the "code is law" ideal collides forcefully with the practical realities of the off-chain world, most acutely through the concept of legal personhood. Legal systems are constructed to govern relationships between "persons", whether they are natural (human beings) or artificial (corporations), that can own property, enter into contracts, sue, and be sued. Operating as a pure technological construct, a native DAO remains unrecognized as a formal legal entity by the vast majority of jurisdictions worldwide. This critical absence of personhood prevents the DAO from being a direct party to legal relations, effectively stripping it of the capacity to engage in foundational economic activities such as owning assets, executing binding agreements with external parties, and accessing the legal system for protection or defense.

The failure of a native DAO to achieve recognized legal status does not, however, mean that it exists in a legal void where the law cannot reach. On the contrary, it creates a dangerous vacuum that the traditional legal system abhors and will inevitably seek to fill by applying the most suitable, or least unsuitable, existing category. When a collective of individuals operates a for-profit enterprise without formally incorporating it into a recognized legal entity, the default classification in most common law jurisdictions is that of a general partnership (Kaal, 2019; Weinstein & Loftchie, 2022).

This default status is catastrophically ill-suited for the typical structure and operation of a DAO. The legal elements required to form a partnership, an association of two or more persons to carry on as co-owners a business for profit, map uncomfortably well onto the activities of many DAOs. Their token holders associate for a common purpose, such as managing a protocol or an investment fund; they act as co-owners through their shared governance rights; and they frequently operate with an expectation that the protocol or its treasury will appreciate in value. By failing to proactively choose a legal form, the participants have one chosen for them by default, and it is a form that carries the single most feared consequence in all of commercial law: unlimited joint and several personal liability. This means that every member of the DAO who participates in its governance could be held personally responsible for the entirety of the DAO's debts and legal obligations (Weinstein & Loftchie, 2022; Zetzsche et al., 2018).

The "joint and several" aspect of this liability is particularly brutal in its application. For instance, if a DAO were to be successfully sued for \$10 million, the plaintiff would not be required to identify and sue all 10,000 of its anonymous token holders. Instead, the plaintiff could identify a single, high-net-worth participant and legally compel that one individual to pay the full \$10 million judgment from their personal assets. It would then fall to that unfortunate individual to attempt the near-impossible task of seeking proportional contribution from thousands of other pseudonymous members scattered across the globe. This level of extreme financial risk is anathema to the culture of passive investment that underpins modern public markets and represents a massive deterrent to mainstream participation in DAOs, thereby stifling innovation and growth (de Oliveira & Rolo, 2023).

5.4.3 Landmark Legal Precedents and the Reality of Liability

This issue has decisively moved from the abstract realm of academic debate and whitepaper theory into the high-stakes arena of the courtroom and regulatory enforcement. The risk of personal liability is no longer a hypothetical contingency but a clear and present danger being actively advanced by both government authorities and private litigants. A recent surge in legal actions demonstrates this trend unequivocally, as regulators have begun to probe the perceived shields of decentralization, while class-action lawsuits increasingly attempt to pierce the veil of code to hold identifiable individuals, from core developers to voting token holders, personally liable for a protocol's failures or financial losses. Each case throws the underlying challenge of legal personality into sharp relief, proving that the abstract legal questions surrounding DAOs are now being tested with real-world, high-stakes consequences. Two landmark legal cases in the United States, *CFTC v. Ooki DAO* and *Sarcuni v. bZx DAO*, have established significant precedents regarding the legal status and liability of DAOs and their members, signaling a clear judicial trajectory towards applying established legal frameworks to these novel digital structures (Bannister, 2021; Commodity Futures Trading Commission, 2023).

In the case of *CFTC v. Ooki DAO*, the U.S. Commodity Futures Trading Commission (CFTC) initiated an enforcement action against the DAO for operating an illegal trading platform that offered leveraged and margined retail commodity transactions without being registered as a designated contract market. A primary legal challenge for the regulator stemmed from the decentralized nature of the Ooki DAO, which lacked a physical address or conventional corporate officers, making the traditional service of process and the direct assignment of liability highly complex (Nathan Vandy, 2024). To overcome this, the CFTC advanced the novel argument that the DAO should be legally recognized as an unincorporated association. Under this classification, the CFTC contended that every token holder who actively participated in the organization's governance by voting on proposals could be considered a member and, therefore, held personally liable for the organization's regulatory violations (Commodity Futures Trading Commission, 2022b). The court ultimately concurred with this reasoning, recognizing the DAO as a "person" under the Commodity Exchange Act and holding it liable for the infractions. Consequently, the court issued a default judgment that included a civil monetary penalty of \$643,542, a permanent trading ban, and an order for the DAO to cease operations and shut down

its website. This ruling established a critical precedent by holding DAO members directly accountable for an entity's actions based on their active participation in its governance.

In a similar vein, the case of *Sarcuni v. bZx DAO* addressed the question of member liability from a different but related legal angle (Bannister, 2021). Following a severe security breach that resulted in approximately \$55 million in losses for users of the protocol, a class-action lawsuit was filed against the bZx DAO. The plaintiffs contended that the DAO operated as a general partnership, which, if established, would make its partners, in this instance, the major token holders and developers, jointly and severally liable for the full extent of the damages (Alexander C. Drylewski, 2023). The court's analysis focused on whether the activities of the bZx DAO met the legal criteria for a general partnership. It found that the plaintiffs had sufficiently demonstrated the core elements: an association of two or more persons (the token holders), the conduct of a business for profit (evidenced by revenue generated from margin trading and lending), and co-ownership and control (exercised through the governance rights attached to the tokens, including voting on proposals and managing treasury funds). The court inferred from these facts that token holders possessing such governance rights were, in effect, partners in the DAO's general partnership (Lee Pascoe, 2023). The implication of this ruling is profound, as general partnerships, by definition, do not offer a liability shield, meaning individual members can be held personally and fully responsible for the entirety of the DAO's liabilities.

Taken together, these cases represent a pivotal shift in the legal treatment of DAOs within the U.S. judicial system. They demonstrate a clear willingness by courts and regulators to look beyond the novel technological structure of DAOs and classify them within existing legal paradigms, thereby exposing individual members to significant personal liability based on their participation in the governance and control of the organization. These decisions have sent a shockwave through the DAO ecosystem, transforming the abstract risk of personal liability into a concrete and demonstrable legal reality. They prove that courts will not be deterred by novel technological structures and will apply long-standing legal principles to hold individuals accountable, regardless of claims of decentralization.

5.4.4 The "Interface Problem": Practical Impediments

In addition to the severe legal challenges discussed above, the lack of recognized legal personality creates a cascade of practical impediments that collectively constitute the "interface problem", the inability of a purely on-chain entity to interact effectively and predictably with the traditional off-chain world. This problem manifests in several critical domains of organizational life.

First is the issue of contractual incapacity. The modern economy operates on a foundation of legally enforceable contracts, but a native DAO cannot be a legal party to one. This limitation cripples its ability to conduct basic business operations. It cannot formally hire core developers or community managers, as employment agreements require a legally recognized employer (Boss, 2023). It cannot lease cloud server space, subscribe to essential software-as-a-service (SaaS) products, or engage an accounting firm for a financial audit, as all of these services are predicated on a legally recognized counterparty that can agree to their terms of service. Every off-chain

relationship becomes legally uncertain and largely unenforceable, forcing reliance on informal agreements with individual contributors who must contract in their personal capacity (Borgogno & Martino, 2024).

Second, a native DAO is incapable of legally owning assets in its own name. While it can control crypto-assets held in its on-chain treasury via smart contracts, it cannot hold legal title to real estate, own the intellectual property (such as copyrights, trademarks, and patents) that underpins its brand and technology, or even open a simple bank account to pay for off-chain expenses in fiat currency (Borgogno & Martino, 2024; Sims, 2019). These crucial off-chain assets must instead be held in the name of individual contributors or a separate, trusted entity, a practice that creates immense legal ambiguity, introduces points of centralization and single-person risk, and fosters a lack of clarity about who truly owns the core components of the project.

Third, the inability to sue or be sued as a single entity renders a DAO legally impotent in disputes. It cannot go to court to enforce a contract against a non-performing vendor or to defend its intellectual property against infringement. Conversely, if a third party has a claim against the DAO, they are forced into the legally complex and aggressive strategy of pursuing individual members, as was demonstrated in the *bZx* and *Ooki DAO* cases, creating a hostile and unpredictable legal environment for all participants (Borgogno & Martino, 2024).

Finally, for tax authorities, a native DAO is a profound puzzle. Its lack of a clear legal form creates deep uncertainty about its tax obligations and status. Is it a partnership, which would require pass-through tax reporting for all members? Is it a corporation, subject to entity-level taxes? Even more fundamentally, where is the DAO located for tax purposes? Is its jurisdiction determined by the physical location of its core developers, the aggregate location of its token holders, the distribution of its server nodes, or some other novel criterion? This ambiguity makes tax compliance nearly impossible and exposes participants to the significant risk of unforeseen and potentially severe tax liabilities (Boss, 2023).

5.5 Limited Liability: The Protective Veil of Modern Enterprise

If legal personality provides the essential skeleton for the modern corporation, then limited liability is its most vital organ. This legal principle transformed the nature of investment from a high-stakes endeavor reserved for the wealthy and intimately connected into a democratized activity accessible to the masses, thereby fueling the single greatest expansion of economic activity in human history. Limited liability is the doctrine that erects an invaluable protective barrier, often referred to as the "corporate veil," between the business entity and its owners. It dictates that an enterprise's creditors can only lay claim to the assets owned by the corporation itself; they cannot seize the personal assets, the homes, savings, or other private property, of the individual shareholders who own the firm. For an investor, this means that their maximum potential loss is strictly and predictably capped at the amount they invested in the company's shares, regardless of the ultimate magnitude of the company's debts or legal liabilities (Easterbrook & Fischel, 1985).

This concept, a cornerstone of modern corporate law, is the direct and most sought-after consequence of the legal personality discussed in the previous section. It is crucial, however, to distinguish it from its conceptual sibling, "entity shielding." While entity shielding protects the corporation's assets from the personal creditors of its shareholders, limited liability, also known as "owner shielding," performs the inverse function: it protects the shareholders' personal assets from the corporation's creditors (Armour et al., 2017). Together, these two principles create a robust legal partition that allows capital to flow into ventures with a clear, calculable, and manageable risk profile.

The development and broad acceptance of limited liability was not a mere legal footnote but a paradigm-shifting event that fundamentally altered the risk calculus for both investment and enterprise. Yet, for all its foundational importance in the traditional corporate world, this essential protection is starkly absent in the native architecture of Decentralized Autonomous Organizations. This absence creates a risk profile so severe that it arguably stands as the single greatest barrier to the mainstream adoption and institutional acceptance of DAOs, forcing participants and developers into a desperate and complex search for legal and legislative solutions to replicate this indispensable corporate shield.

5.5.1 The Corporate Paradigm: The Economic Rationale for Shielding Owners

The modern investment landscape is so thoroughly defined by the principle of limited liability that it is difficult to envision a world without it. Before its widespread adoption in the 19th century, the dominant legal form for joint enterprise was the general partnership. In that model, every partner was fully and personally liable for all the debts of the business. An investment in any enterprise was therefore a "bet-the-farm" proposition; a single business failure, regardless of its cause, could lead to complete personal ruin. This unforgiving legal environment naturally suppressed both the scale of investment and the number of willing investors. Only those who could afford to lose everything, or those who were so intimately involved in the management of a venture that they could closely monitor its every risk, would dare to participate.

The introduction of limited liability changed everything. Its evolution was gradual, moving from a complete absence in the 17th and 18th centuries, through various hybrid and charter-based regimes, to its eventual status as a default, uniform attribute of the modern corporation (Biyan Mienert, 2024; Harris, 2020). This legal innovation acted as a powerful economic catalyst for several key reasons. First, by capping the downside risk for investors, limited liability made them willing to provide capital at a lower cost. This encouraged investment in new, innovative, but inherently risky ventures, the very engines of economic progress, that might otherwise have never been funded.

Second, it facilitated the critical practice of diversification. Limited liability allowed investors to hold smaller stakes in numerous companies without needing to become an expert in the operations of any of them or to closely monitor their every action (H. G. Manne, 1967). Without this protection, a rational investor would have to expend enormous resources to intensively monitor the management of every single company in their portfolio to protect their personal wealth from

the consequences of a single firm's failure. With it, they could safely diversify their holdings across a wide range of assets, reducing their overall risk and encouraging broader participation in capital markets (Florian Möslin & Daniel Ostrovski, 2024).

Third, and perhaps most importantly, limited liability was an essential prerequisite for the development of modern, liquid public markets. It achieves this by making shares fungible, that is, ensuring that one share of a company is economically identical to any other. If liability were unlimited, the value of a share would depend not only on the company's performance but also on the personal wealth of every other shareholder who could be called upon to cover its debts. This would make shares non-fungible and trading them an impossibly complex undertaking. By severing this link between corporate performance and the personal wealth of shareholders, limited liability allowed for the impersonal, high-volume, and efficient trading that characterizes liquid capital markets today.

Initially, the landmark 1897 English case of *Salomon v Salomon & Co Ltd* solidified the principle, affirming that even a single individual could form a corporation to create a separate legal entity and benefit from a liability shield, cementing its place at the very core of corporate law (Puig, 2000; Sims, 2019). Then, the adoption of this principle was accelerated by fierce jurisdictional competition; as some states or nations began offering limited liability, others were compelled to follow suit for fear of "capital flight," as businesses and investors migrated to more favorable legal environments (Sims, 2019).

5.5.2 The Inherent Trade-Off: Moral Hazard and Creditor Protection

However, the powerful benefits of limited liability are not without their costs. By shielding shareholders from the full consequences of corporate failure, the doctrine shifts a significant portion of the enterprise's risk onto the corporation's creditors. This risk transfer is particularly acute for involuntary creditors, such as tort victims, for example, individuals harmed by a company's defective product or a community affected by its environmental pollution, who do not choose to engage with the company and are in no position to negotiate for contractual protections beforehand.

This risk-shifting dynamic creates a classic moral hazard problem. Because shareholders are positioned to reap all the rewards of successful, high-risk strategies but are shielded from the catastrophic losses of failure, they have a structural incentive to cause the corporation to take on excessive levels of risk. They are, in effect, gambling with their creditors' money. To counterbalance this inherent incentive for risk-taking, *corporate law* has developed a crucial set of *protective mechanisms* designed to maintain fairness and systemic stability. Historically, these included *minimum capital requirements*, which compelled companies to maintain a baseline financial buffer to protect creditors from total loss. Over time, these safeguards evolved to include more sophisticated *fiduciary duties*, which legally oblige directors and officers to act in the best interests of the corporation as a whole, balancing the interests of shareholders, creditors, and other stakeholders. In parallel, *mandatory financial disclosure regimes* emerged to ensure transparency, providing creditors and investors with the information necessary to evaluate a firm's financial

health and risk exposure. Finally, in extreme cases where the corporate form has been misused, such as when owners exploit limited liability to perpetrate fraud or gross injustice, courts can invoke the doctrine of “*piercing the corporate veil*” to hold shareholders personally liable for corporate misconduct (Biyan Mienert, 2024; Brummer & Seira, 2022). These layered protections form a comprehensive legal safety net that counteracts the moral hazards inherent in limited liability and ensures the integrity of corporate governance.

5.5.3 The Native DAO: A Return to an Era of Unlimited Liability

The native, unincorporated DAO, which operates purely as code on a blockchain, inadvertently casts its participants back into the high-risk legal world that existed before the widespread adoption of the modern corporate form. As previously established, the failure of a DAO to secure formal legal personality from the state results in its default classification as a general partnership in most common law jurisdictions (Weinstein & Loftchie, 2022). This default status is not a neutral placeholder; it is a legal determination that carries the draconian consequence of unlimited, joint, and several liability for every participating member (Weinstein & Loftchie, 2022).

For a DAO participant, this means that the simple act of using their tokens to vote on a governance proposal could be legally interpreted as acting as a partner in a for-profit enterprise. This single act could, in turn, expose them to personal liability for the entirety of the DAO's debts and legal obligations. This liability is not confined to predictable contractual debts; it can extend to damages arising from catastrophic smart contract hacks, user losses due to protocol failures, claims of intellectual property infringement, or substantial fines levied for regulatory violations (Sims, 2019). This terrifying and unpredictable risk profile stands as a major obstacle to the development and growth of DAOs, as few rational actors would be willing to expose their entire personal wealth for the potential upside of participating in a decentralized project (Sims, 2019). The legal actions against Ooki DAO and bZx DAO serve as stark, real-world confirmations of this danger. As previously mentioned, in the Ooki DAO case, a U.S. regulator successfully advanced the theory that voting token holders were members of an unincorporated association and were therefore personally liable for its violations (Commodity Futures Trading Commission, 2023). Similarly, the lawsuit against bZx DAO was constructed upon the allegation that it operated as an unincorporated partnership, with the explicit goal of holding its members jointly and severally liable for user losses (Lee Pascoe, 2023). These cases unequivocally demonstrate that the legal system will not hesitate to apply this default classification, turning a theoretical risk into a tangible and severe threat.

5.5.4 The Failure of "Code is Law" as a Liability Shield

Proponents of a pure, technologically-determinist view of DAOs initially hoped that the "code is law" ethos could create a self-contained and self-regulating system that would operate outside the reach of traditional legal liability frameworks (Borgogno & Martino, 2024). The argument was that if all organizational rules are encoded in an open and transparent smart contract, then all

participants are fully aware of the operational logic, and the automated execution of that code should be the final and binding word on all matters. However, this perspective fundamentally misunderstands the nature and sovereignty of law. A state-granted liability shield is a public policy decision, a legal privilege conferred by a sovereign authority; it is not a technical feature that can be replicated or substituted with cryptographic code. While a smart contract can create a form of *technical* capital lock-in, it cannot, on its own, create *legal* entity shielding or owner shielding, as these concepts require the affirmative intervention and recognition of an external legal system (Borgogno & Martino, 2024).

The law exists separately from and externally to the blockchain, and it will impose its own rules and norms upon the activities that occur on-chain, especially when those activities have real-world consequences. A court of law will not accept a smart contract as a substitute for a legally recognized corporate form when it comes to assigning liability for harm caused to a third party. The "code is law" argument often fails to account for the higher-level goals of civil liability systems, which include crucial social functions such as compensating victims, deterring harmful behavior, and upholding important public policies like consumer and environmental protection (Peder Østbye, 2024). The legal system is designed to achieve these objectives and will not be displaced by a purely technical architecture.

This disjunction between legal and technical systems also results in the absence of several key protections that corporate law traditionally affords to shareholders. As explained in the preceding section, corporate law has evolved a complex set of mechanisms, such as fiduciary duties, disclosure obligations, and the doctrine of piercing the corporate veil, to curb excessive risk-taking and prevent abuses of power. These safeguards ensure accountability within a legally recognized corporate structure and provide recourse for parties harmed by mismanagement or opportunism. By contrast, DAOs operate outside the framework of corporate law and therefore lack these institutionalized protections. In most jurisdictions, DAOs are not recognized as legal persons, and their participants are not shielded by the traditional doctrines of limited liability, fiduciary obligation, or minority shareholder protection. Instead, DAO governance is determined primarily by *code-based rules* encoded in smart contracts and *token-weighted voting mechanisms*, which often privilege majority token holders at the expense of smaller participants. Without a legal board of directors or fiduciary oversight, majority actors can unilaterally pass proposals, modify governance parameters, or even reallocate treasury assets, leaving minority token holders with no meaningful recourse. Moreover, the absence of statutory *disclosure obligations* or external auditing requirements further erodes transparency, making it difficult for participants to assess financial risks or detect governance abuse.

In this unregulated environment, the *principles of corporate accountability and fairness* that traditionally protect shareholders and creditors are effectively absent. Minority token holders in DAOs cannot rely on courts to intervene against oppressive governance actions, nor can they invoke doctrines such as fiduciary breach or veil-piercing to challenge bad-faith conduct. Instead, they are bound by the deterministic logic of the smart contract, "code is law", which provides procedural certainty but little substantive justice. This asymmetry reveals a profound governance gap: while corporations internalize risk through a mature system of checks and balances grounded in law, DAOs externalize risk to their participants, relying on voluntary norms and community consensus rather than enforceable legal protections. As a result, unless regulatory innovations or

hybrid legal structures emerge to extend similar safeguards to decentralized entities, DAOs will remain inherently more precarious environments for minority participants and counterparties alike.

5.5.5 Broader Implications and the Path Forward

The intense debate surrounding limited liability for DAOs represents a classic policy balancing act. On one hand, granting a robust liability shield is essential to protect the personal assets of participants, which in turn encourages the risk-taking and innovation that drives the entire ecosystem forward (Biyani Mienert, 2024). It also facilitates the necessary integration of DAOs into existing legal and commercial systems, allowing them to interact with traditional entities with greater certainty and less friction (Biyani Mienert, 2024). On the other hand, this protection cannot be absolute or unconditional. It must be carefully balanced with robust mechanisms for creditor protection to prevent the same moral hazard problems that have been observed and managed in the corporate world for over a century. To this end, novel proposals are emerging that seek to create this balance in a DAO-native context. These include concepts such as requiring DAOs that benefit from a liability shield to maintain independent liability funds, perhaps through mandatory insurance or by algorithmically allocating a portion of treasury assets, to ensure that there is an identifiable and solvent source of funds to compensate creditors and tort victims (Biyani Mienert, 2024).

Furthermore, a key argument in favor of establishing a clear, entity-level liability regime is the sheer inefficiency and ineffectiveness of the alternative. The pseudonymity and global dispersion of DAO members make the prospect of identifying and successfully enforcing judgments against thousands of individual token holders a practical impossibility for most creditors. In this context, the threat of unlimited personal liability functions less as a viable means of creditor protection and more as a powerful and indiscriminate deterrent to participation and governance (Schwemmer, 2023). This suggests that a well-regulated, entity-level approach is ultimately superior for all parties involved, as it would provide essential legal clarity for participants while offering a more realistic and efficient path to recovery for creditors.

In the final analysis, limited liability is a state-granted privilege, not an inherent technological feature that can be coded into existence. For the modern corporation, it was the pivotal legal innovation that unlocked global capital markets and enabled an unprecedented era of economic growth. For the native DAO, its absence represents a dangerous regression to a more perilous period of commerce, exposing participants to risks that are both unacceptable to individuals and unsustainable for the ecosystem as a whole. The frantic search for a liability shield, through the imperfect compromise of legal wrappers and the promising but fragmented frontier of bespoke legislation, highlights the central tension between the decentralized, borderless world of blockchain technology and the territorially-bound, state-centric nature of law.

Having established the critical importance of a liability shield to protect the owners of a decentralized enterprise, the next logical step in constructing a viable organizational model is to ensure that the ownership stakes themselves are liquid and easily transferable. The corporate share is the quintessential example of such an instrument, providing the foundation for modern capital

markets. We now turn to an analysis of how DAOs, through the mechanism of cryptographic tokens, have radically reimagined the concept of transferable shares, creating both unprecedented liquidity and a host of novel regulatory challenges.

5.6 Tokens as Transferable Shares

One of the most enduring and economically significant features of the corporate form is the principle of transferable ownership interests. In the corporate context, shares of stock are designed to be freely tradable instruments that allow investors to fluidly adjust their portfolios, exit their investments, or enter new ones without undermining the legal existence or operational stability of the firm itself. This capacity for transferability is what sustains vibrant secondary markets, supports investor confidence, and underpins the ability of corporations to raise capital effectively from a wide and dispersed pool of investors (Kraakman et al., 2017). Transferability thus functions not merely as a convenience for investors but as a core structural mechanism that fosters liquidity, facilitates diversification, and enables the continuous process of price discovery that anchors modern financial markets.

For Decentralized Autonomous Organizations, the functional equivalent of the transferable share is the cryptographic token. Tokens constitute the primary medium through which rights, responsibilities, and ownership stakes in a DAO are allocated, managed, and exercised. The very architecture of blockchain technology was constructed with the seamless and secure transfer of digital assets in mind, and DAOs have leveraged this foundational feature to design ownership mechanisms that are frictionless, transparent, and inherently global in scope (Borgogno & Martino, 2024). Transferability is arguably even more central to the nature of DAOs than it is to traditional corporations, because for a DAO, the token constitutes both the infrastructure for community governance and the primary mechanism through which economic value is created and exchanged. This section examines transferable shares in corporations and transferable tokens in DAOs as parallel, yet distinctly different, organizational mechanisms. By analyzing the nature of the ownership asset, the processes of transfer and record-keeping, and the implications for market liquidity and governance, this discussion will highlight both the continuities and the disruptive divergences between the traditional corporate form and the emergent DAO model.

5.6.1 The Nature of the Ownership Asset

In the corporate setting, ownership is traditionally expressed through shares of stock. These shares are intangible property rights that entitle their holders to a legally defined bundle of benefits under corporate law. Depending on the specific class of shares, these rights may include the power to vote in shareholder meetings, the right to receive dividend distributions, and the claim to a share of residual assets upon the corporation's liquidation (J. G. Allen, 2020). Corporate shares are structured into standardized forms by corporate laws, such as common stock or preferred stock, each with a predictable and legally enforceable set of rights and obligations (Biyan Mienert, 2024).

Critically, every share within the same class is typically fungible, meaning that it carries the exact same rights and value as any other share of that class (Sims, 2019). This uniformity is a vital feature of the corporate model because it allows for clear valuation, facilitates mass trading on public stock exchanges, and supports the processes of large-scale capital raising.

By contrast, the ownership asset in a DAO is the token. Tokens are digital assets created and managed on a blockchain, and they may serve a diverse array of purposes that extend far beyond the narrow financial role of traditional shares. DAO tokens can represent governance rights, economic claims, or rights of access to particular services within the ecosystem (Wright, 2021). They frequently combine these functions in novel and complex ways, producing hybrid assets that do not map neatly onto traditional corporate categories (Borgogno & Martino, 2024). They are also largely unconstrained by regulatory definitions, allowing developers to design tokens with virtually any combination of features or rights they choose to embed. For instance, a governance token may confer upon its holder the right to propose and vote on changes to the protocol, while simultaneously appreciating in value if the DAO's ecosystem grows and thrives. In other cases, tokens may provide specific utility functions, such as granting access to decentralized platforms, alongside more conventional investment-like features.

This fusion of functions makes DAO tokens inherently more flexible but also significantly more complex than corporate shares. Whereas a share primarily expresses a claim on a company's profits and residual value, a token often constitutes a multi-dimensional package of rights, blending participation, governance, and utility into a single instrument. This diversity of design makes DAO tokens inherently resistant to uniform legal treatment. Unlike standardized corporate shares, whose rights and obligations are clearly defined within established statutory frameworks, DAO tokens exist along a shifting continuum of economic and governance functions. Their hybrid and evolving nature defies the categorical assumptions upon which corporate regulation is built, making them exceedingly difficult to capture within any existing body of corporate law or securities regulation.

5.6.2 Mechanisms of Transfer and Record-Keeping

The efficiency and integrity of ownership transfer is a central concern in both corporate and decentralized organizations, but the technological underpinnings of each system differ markedly, revealing a fundamental divergence in their philosophies of trust and intermediation. In the traditional corporate world, transfers of shares are meticulously recorded through official registries maintained either by the company itself or, more commonly, by a web of trusted intermediaries such as transfer agents and custodians. Particularly in large, publicly listed corporations with millions of shareholders, these processes are inherently complex, costly, and opaque to outsiders. Maintaining accurate shareholder ledgers, processing share transfers in compliance with securities laws, and verifying ownership for corporate actions can involve significant and ongoing expenditures on administrative staff, legal counsel, and a host of third-party service providers (Beckett, 2023). Even with the extensive digitization of modern financial markets, the core infrastructure of share transfer remains a mediated process, reliant on layers of centralized institutions and subject to extensive regulatory oversight.

DAOs, by contrast, leverage the native properties of blockchain technology to manage the issuance, transfer, and record-keeping of tokens in a radically different manner. Each token transfer is recorded as a transaction on a distributed, immutable ledger, a process that entirely eliminates the need for centralized registries or manual verification by a trusted third party (Weinstein & Loftchie, 2022). Because the blockchain itself, through its consensus mechanism and cryptographic security, guarantees the authenticity and chronological integrity of every transfer, the administrative costs associated with record-keeping are dramatically reduced, while transparency is significantly enhanced. In practical terms, a DAO can facilitate the near-instantaneous transfer of ownership stakes among thousands or even millions of global participants at a near-zero marginal cost, without requiring the involvement of lawyers, custodians, or other intermediaries that are indispensable to the corporate system (Beckett, 2023).

The contrast is particularly stark when considering how each system achieves global scale. Corporations achieve scale by constructing complex, interlocking networks of trusted institutions, stock exchanges, clearing houses, and regulatory authorities, that work in concert to maintain confidence and integrity in the system. DAOs achieve a comparable, if not greater, scale through the inherent architectural properties of blockchain technology itself: cryptographic verification, distributed consensus, and the automated execution of rules via smart contracts. These mechanisms are not only cheaper and more efficient but are also far more transparent, as every token transfer can be independently verified in real time by any network participant. Moreover, the design of token transfers is not limited to mimicking traditional share sales. DAOs can program novel distribution mechanisms, such as "airdrops," in which tokens are distributed freely to community members as incentives for participation or as rewards for past loyalty (Sims, 2019). Such mechanisms have no direct corporate equivalent and underscore how DAOs use the programmable nature of digital assets to fundamentally rethink the logic of ownership transfer and community formation.

5.6.3 Acquisition and Distribution of Ownership Interests

The pathways through which ownership interests are initially created and subsequently distributed reveal further sharp contrasts between the centralized, structured world of corporations and the more fluid, decentralized ecosystem of DAOs. In the conventional corporate model, ownership interests are created and allocated through the formal issuance of shares. At the earliest stages of a company's life, these shares are distributed to founders, early investors, and key employees through private agreements, often supplemented by stock option plans. As companies mature and seek to raise additional capital, they may pursue public offerings, such as an *Initial Public Offering (IPO)*, a process that involves extensive regulatory scrutiny, the participation of underwriters, and a formal listing on a recognized stock exchange (Easterbrook & Fischel, 1996). Each issuance of new shares must comply with a thicket of securities regulations and mandatory disclosure requirements, and the process typically involves substantial financial and legal advisory costs. The distribution of corporate ownership is therefore a centralized, highly structured, and heavily mediated affair, guided by well-established financial institutions and legal norms.

DAOs, however, frequently adopt alternative and more decentralized methods of token distribution. The first common model is the token sale, called Initial Coin Offering (ICO), in which individuals contribute cryptocurrency to the project in exchange for newly minted DAO tokens. This mechanism functions as a form of global, permissionless fundraising campaign that can attract a broad participant base in a very short timeframe (Weinstein & Loftchie, 2022). Another method that is gaining prominence is the allocation of tokens as direct compensation for labor or services provided to the DAO, a practice that directly links the distribution of ownership to tangible contributions made to the community, thereby fostering a strong sense of shared enterprise (de Sousa, 2024).

Beyond these parallels to corporate issuances, DAOs frequently employ the unique tool of the *airdrop*. This involves distributing tokens free of charge to existing or potential participants, often as a reward for early support of the project, active community involvement, or even as part of a randomized distribution to attract new users (Sims, 2019). This democratization of ownership distribution has important consequences. Whereas acquiring a meaningful ownership stake in a corporation generally requires an investor to commit significant financial capital, DAOs can grant ownership as a byproduct of active participation or demonstrated loyalty. This dramatically lowers the threshold for entry, broadening the potential ownership base far beyond the traditional investor class. At the same time, this approach can create significant challenges for ensuring sustained engagement, as recipients of freely distributed tokens may lack the long-term financial or ideological commitment to align with the DAO's objectives. Nevertheless, the diversity of these distribution methods highlights how DAOs use programmable digital assets to expand the conceptual boundaries of ownership allocation, blurring the lines between investment, labor, and community participation.

5.6.4 Liquidity, Exit, and Market Dynamics

Liquidity is another critical area where corporate shares and DAO tokens exhibit both continuity in principle and divergence in practice. Publicly traded corporations have developed highly liquid markets for their shares, facilitated by a global infrastructure of stock exchanges, brokers, and a vast array of other financial intermediaries. Shares of large corporations can be bought and sold almost instantaneously, often in enormous volumes, with prices that reflect the continuous aggregation of information and the dynamics of supply and demand. However, it is crucial to note that shares of private corporations are far less liquid. Transfers of ownership in such entities often require approval from other shareholders or must comply with restrictive shareholder agreements, making the process of exiting an investment far more difficult and costly (Sims, 2019). Again, the *sale and transfer of shares* are subject to stringent statutory and procedural requirements, particularly in the case of publicly traded companies, where securities regulations impose disclosure, registration, and compliance obligations to safeguard market integrity and investor protection.

DAO tokens, by contrast, are typically designed for liquidity from their very inception. Because they are recorded on a public blockchain, tokens can be traded directly on decentralized exchanges (DEXs) without the need for centralized intermediaries and without any strict regulatory

requirements¹⁹ (Borgogno & Martino, 2024). This peer-to-peer trading model allows participants to enter and exit their positions at will, creating an exceptionally fluid ownership structure with minimal technical or administrative barriers to transfer. The inherent liquidity of DAO tokens also facilitates rapid and continuous price discovery, as token values can fluctuate in real time based on shifting perceptions of the DAO's performance, the effectiveness of its governance, or broader external market conditions.

A particularly distinctive feature of DAOs is the mechanism of *forking*, a form of organizational exit that is entirely absent in the corporate world. Unlike in a corporation, where dissatisfied shareholders are generally limited to selling their shares or campaigning for a change in management, participants in a DAO can collectively "*exit*" by duplicating the organization's open-source codebase and creating a new, independent version of the organization with a modified set of rules. This practice allows communities to resolve intractable disagreements by splitting rather than by forcing a divisive consensus, representing a novel form of organizational mobility. Forking not only enhances the bargaining power of minority participants but also creates a constant competitive pressure within the ecosystem, incentivizing DAOs to maintain alignment with the interests of their members.

Still, the promise of frictionless liquidity in DAOs is not without its own challenges. While token trading is technologically seamless in principle, the potential for a high concentration of tokens in the hands of a few large holders, or "whales," can significantly distort market dynamics and governance outcomes. Moreover, because many DAOs continue to operate without a recognized legal personality, institutional investors, the bedrock of deep, stable capital markets, may hesitate to participate despite the clear liquidity advantages, thereby curbing the potential depth and long-term stability of these markets (Weinstein & Loftchie, 2022). These frictions demonstrate that while DAOs may surpass traditional corporations in the technological ease of ownership transfer, they also face unique and formidable obstacles in their journey toward sustaining robust, mature, and trustworthy liquid markets.

5.6.5 Rights Conferred by Ownership Interests

The specific rights conferred through ownership interests are perhaps the most critical dimension for comparing transferable shares and tokens, as they fundamentally shape the nature of governance, economic participation, and the alignment of interests within an organization. In the corporate world, shareholder rights are relatively standardized and clearly delineated by centuries of legal precedent and statutory law. Shareholders typically enjoy voting rights on a limited set of fundamental decisions, such as electing the board of directors or approving major corporate restructurings like mergers and acquisitions. However, the vast authority over day-to-day management and strategic execution is formally delegated to professional executives and the directors who oversee them, leaving shareholders with limited direct involvement in the company's affairs (Mondoh et al., 2022). Their economic rights usually take the form of dividends, which are

¹⁹ It should be noted that the SEC and CFTC have recently placed increasing scrutiny on the sale of tokens, particularly in the context of Initial Coin Offerings (ICOs).

distributed at the discretion of the board, or residual claims on the company's assets in the event of a liquidation. In short, corporate shares grant a form of indirect governance power and a set of contingent economic rewards, with both heavily mediated by the fiduciary duties of managers and the strictures of statutory regulation (Kraakman et al., 2017).

DAO tokens, in contrast, often bundle a broader and more flexible set of rights, with a strong emphasis on direct participation. Governance tokens grant their holders the ability to directly submit, deliberate upon, and vote on proposals, thereby participating in the strategic and operational direction of the organization (Weinstein & Loftchie, 2022). Unlike corporate voting, which is largely confined to high-level, periodic matters, DAO governance may extend to a wide array of granular, operational questions, such as treasury allocations, protocol upgrades, hiring decisions, or even the establishment of community norms. This model of direct involvement is often framed as a native solution to the principal-agent problem that plagues corporations, as the need for intermediating managers is theoretically reduced or eliminated (Florian Möslin & Daniel Ostrovski, 2024).

While voting rights in DAOs are frequently proportional to token holdings, resembling the one-share-one-vote principle common in corporations, the DAO ecosystem is also a fertile ground for experimentation with alternative voting models. Mechanisms such as quadratic voting, one-person-one-vote systems, and delegated voting (often termed "liquid democracy") have been tested as methods to counterbalance the concentration of power in the hands of large token holders and to promote a fairer representation of diverse community interests (Hassan & De Filippi, 2021). Such experimentation has no direct analogue in the more rigid world of corporate governance, where voting rights are more narrowly and statutorily defined.

The economic rights associated with DAO tokens are likewise more fluid and less legally defined. Rather than receiving periodic, board-approved dividends, token holders may realize economic gains primarily through the appreciation of their tokens' value on secondary markets or through direct, token-based distributions from the DAO's treasury as approved by a community vote (Borgogno & Martino, 2024). Additionally, when DAOs pay contributors or service providers in their native tokens, recipients gain not only compensation for their labor but also a direct ownership stake in the enterprise, creating a powerful, recursive cycle of participation and stakeholding (de Sousa, 2024). This blurring of the lines between labor compensation and ownership participation distinguishes DAOs sharply from traditional corporations, where wage labor and shareholder ownership are typically maintained as distinct and separate categories. Overall, DAO tokens fundamentally reimagine the *"bundle of rights"* associated with corporate shares by combining governance, economic, and participatory functions into a single, programmable digital instrument. While this integration can foster powerful alignment and inclusivity, it also complicates valuation and regulation, since these multi-faceted tokens do not fit neatly into the established legal categories of equity, debt, or utility.

5.6.6 Transferable Ownership

The nature of transferable ownership interests is not merely a financial feature; it is a structural force that directly shapes the governance and organizational dynamics of an enterprise. In corporations, the ability to freely transfer shares ensures that ownership and control can remain distinct. Shareholders can adjust their investment portfolios without destabilizing the firm's managerial structure, while professional managers continue to exercise their delegated authority. This formal separation of ownership and control has been one of the defining characteristics of the modern corporation, enabling it to achieve immense scale and operational effectiveness (Kraakman et al., 2017).

In DAOs, however, the very transferability of tokens directly and immediately influences the governance dynamic. Because tokens often confer direct governance rights, the transfer of tokens is equivalent to the transfer of political influence within the organization. An individual or entity that accumulates a large number of tokens through purchases on secondary markets simultaneously gains a proportionate degree of control over the DAO's future direction. Conversely, participants who sell their tokens relinquish not only their economic stake but also their voice and voting power in the community. This tight coupling of financial interest and governance power differentiates DAOs from corporations, where passive investors can readily sell their shares without directly affecting the continuity of the firm's management.

This model of direct, token-based governance also exposes DAOs to a new set of risks. Just as large shareholders in a traditional corporation can exert disproportionate influence, so too can "whales" in a DAO accumulate vast power by holding large quantities of tokens. This creates the ever-present possibility of oligarchic control in what is, by intention, supposed to be a decentralized structure (Weinstein & Loftchie, 2022). To mitigate this risk, DAOs are actively experimenting with novel governance mechanisms such as quadratic voting or systems of time-locked tokens that reward and empower long-term commitment rather than speculative accumulation (Hassan & De Filippi, 2021). Such mechanisms demonstrate both the flexibility and the fragility of DAO governance: flexibility, because they can design and deploy novel voting systems that are impossible in the corporate world, and fragility, because these systems remain largely untested at scale and are potentially vulnerable to new forms of manipulation and attack.

Another organizational implication of this model lies in the realm of inclusivity. Traditional corporations, by their nature, tend to exclude non-shareholder stakeholders like employees and customers from formal ownership, unless explicit and often complex mechanisms, such as employee stock option plans, are created. DAOs, by contrast, can readily and frictionlessly expand participation by distributing tokens to contributors, users, or even entire communities through mechanisms like airdrops or ongoing reward systems (Sims, 2019). This feature can foster a powerful sense of community ownership and shared purpose, but it also fundamentally blurs the lines between previously distinct stakeholder categories. The result is a novel organizational form that is simultaneously more inclusive and potentially more fragmented, as its diverse participants may hold widely differing and sometimes conflicting motivations' some being primarily financial, others primarily ideological or utilitarian.

5.6.7 Theoretical and Economic Perspectives

From a theoretical standpoint, the principle of transferability can be situated within the framework of transaction cost economics. Ronald Coase's seminal insight was that firms exist primarily to reduce the costs associated with conducting transactions in an open market (Coase, 2012). In the corporate context, transferable shares serve to reduce transaction costs for investors by creating a liquid market for ownership stakes, enabling individuals to reallocate their capital efficiently without having to renegotiate the complex web of contractual relationships that constitute the firm. Oliver Williamson later expanded upon this framework, highlighting how corporate governance structures are designed to balance the trade-offs between hierarchical control and market efficiency (Riordan & Williamson, 1985).

DAOs reconfigure this classic economic equation by leveraging blockchain technology to minimize transaction costs even further. The peer-to-peer transfer of tokens requires no intermediaries, clearing houses, or centralized registries. Smart contracts execute these transfers automatically and securely, reducing the coordination costs associated with changing ownership to a negligible level (Borgogno & Martino, 2024). This radically lowers the threshold for global participation, as individuals anywhere in the world can buy, sell, or earn ownership stakes without having to navigate complex and costly institutional infrastructures. In effect, DAOs extend Coase's theory by demonstrating how new digital technologies can collapse traditional organizational boundaries and begin to replace hierarchical management with more fluid, market-like governance mechanisms.

The functions of liquidity and price discovery also illustrate this theoretical transformation. In the corporate world, capital markets serve as vast arenas where information about a firm's performance, prospects, and management quality is aggregated and reflected in its share price. In DAOs, token markets serve a similar function, but the scope of information being priced is often broader and more complex. Token values may reflect not only financial performance metrics but also community perceptions of governance quality, protocol security, the strength of network effects, or even the organization's social and ideological reputation. This convergence of economic and social signals within the valuation of a single token complicates the pure efficiency of price discovery but also highlights how DAOs uniquely embed their governance dynamics directly into their market mechanics.

5.6.8 Brief Regulatory Note

While this section emphasizes the comparative organizational features of transferability, it is essential to briefly note that this characteristic has profound and unsettled regulatory implications. Corporate shares are universally recognized as securities and are embedded within mature and well-understood legal frameworks that govern their issuance, trading, and disclosure requirements. DAO tokens, by contrast, often straddle multiple legal categories, creating significant uncertainty. In the United States, the Securities and Exchange Commission has frequently sought to treat governance tokens as securities, applying the venerable *Howey test* to determine whether they

constitute an *"investment contract"* where purchasers rely on the efforts of others for profit (Dimitropoulos, 2020). In the European Union, *the Markets in Crypto-Assets Regulation (MiCA)* creates new, harmonized categories for utility and asset-referenced tokens but explicitly avoids defining DAOs or providing clear rules for governance tokens, leaving a significant regulatory gap (Borgogno & Martino, 2024).

This legal ambiguity matters immensely because the practical ease of transferability is inseparable from legal recognition and certainty. Corporate shares enjoy frictionless transfer in liquid markets precisely because their legal status is clear and undisputed. DAO tokens, while technologically designed for seamless transfer, often face significant barriers to broader institutional acceptance because of these unsettled regulatory classifications. For now, DAOs exist in a liminal space where their technological capacity for transfer is unmatched, but the legal and regulatory certainty that underpins corporate share transfer remains superior.

5.6.9 Conclusion on Transferable Interests

The comparison of transferable shares and DAO tokens reveals both striking parallels and transformative differences. In corporations, transferable shares are the bedrock of liquidity, investor confidence, and efficient capital allocation. They are standardized, legally defined instruments backed by clear regulatory recognition, designed to support large-scale capital markets and a stable governance model built on delegated management. Their easy transferability ensures that ownership can circulate freely without destabilizing the organization's operational continuity, thereby sustaining the crucial separation of ownership and control that defines modern corporate governance.

In DAOs, tokens inherit the core principle of transferability but radically reimagine its purpose and scope. They combine economic, governance, and utility functions into a single, programmable digital asset, enabling not just financial participation but also direct and continuous involvement in organizational decision-making. Their transfer is facilitated by blockchain technology, which dramatically reduces costs, enhances transparency, and introduces novel distribution and exit mechanisms like airdrops and forking. These features expand inclusivity and fluidity but also introduce new risks of power concentration, governance instability, and regulatory ambiguity. From an organizational perspective, transferable tokens blur the boundaries between investor, participant, user, and worker, creating dynamic communities where ownership is both broader and more fragmented than in traditional corporations. From a theoretical lens, they push transaction cost economics to its technological frontier, reducing coordination costs to near zero while deeply embedding governance within market dynamics.

In sum, transferability in DAOs is not merely a replication of corporate shares in a new digital form. It represents a fundamental reconfiguration of the concepts of ownership, governance, and participation, with implications that extend far beyond the realm of finance. While corporations and DAOs both share a structural reliance on transferable interests, the ways in which these interests are conceived, distributed, and exercised diverge in profound and challenging ways. The great task ahead for lawmakers and legal scholars lies in reconciling these powerful technological

innovations with the stability, predictability, and legal certainty that corporate law has long provided. Having analyzed how ownership stakes are defined and transferred, the next critical element of organizational design is how decisions are made and by whom. This brings us to the core principle of delegated management.

5.7 Delegated Management from Human Agents to Algorithmic Execution

At the very core of the modern corporation lies a fundamental compromise, a pragmatic solution to the otherwise impossible complexity of large-scale enterprise: the principle of delegated management. This principle signifies the formal and legal separation of ownership from control, a structure wherein thousands, or even millions, of disparate shareholder-owners entrust the stewardship of their collective capital to a specialized group of professional managers and a board of directors tasked with their oversight (Kraakman et al., 2017). This delegation is not merely an incidental feature of corporate design; it is the essential mechanism that enables vast pools of passive capital to be aggregated and directed by expert decision-makers, making it possible to construct and sustain organizations of a scale and complexity that would be unimaginable under a model of direct owner-management.

However, this efficient division of labor gives rise to the central and enduring dilemma of corporate governance: the principal-agent problem. By creating a distinct class of agents (managers) whose interests may diverge from those of the principals (shareholders), the corporate form institutionalizes a potential conflict that, in turn, requires a vast and costly apparatus of legal and market-based constraints, from legally imposed fiduciary duties to complex incentive contracts, to monitor and mitigate (Jensen & Meckling, 2019). For over a century, this model of delegated authority, with all of its inherent tensions and the legal framework designed to contain them, has been the undisputed paradigm for organizational management in the global economy.

It is into this established order that the Decentralized Autonomous Organization emerges, not as an incremental improvement upon the existing model, but as a radical ideological and architectural assault on the very concept of delegated management. The foundational promise of the DAO is to resolve the principal-agent problem not by better regulating the agent, but by eliminating the agent entirely (Morrison et al., 2020). It seeks to replace the opaque, trust-based hierarchy of the boardroom with a transparent, "trustless" system of direct governance, where ownership and control are re-bundled, and where decisions are proposed, voted upon, and automatically executed by a distributed network of token holders (Sims, 2019). This section dissects the profound chasm between these two competing models of management. First, it will explore the corporate paradigm, examining the economic rationale for delegation and the legal framework meticulously designed to contain the inescapable agency costs it creates. Second, it will analyze the DAO's revolutionary alternative of direct, algorithmically, enforced governance, evaluating both its powerful theoretical appeal and the significant practical challenges that have emerged in its application.

5.7.1 The Corporate Paradigm: The Efficiency and Dilemma of the Agency Relationship

The hierarchical structure of the modern public corporation is a direct and logical response to the immense coordination and information costs that would otherwise paralyze an organization managed directly by its dispersed owners. In a firm with thousands of shareholders scattered across the globe, a system of direct democracy is not just inefficient; it is a practical impossibility (Kraakman et al., 2017). Each shareholder would need to invest an untenable amount of time and resources to become sufficiently informed on the constant stream of complex operational, financial, and strategic decisions required to run a large enterprise. The transaction costs associated with convening, debating, and achieving consensus among such a large and heterogeneous group would be astronomical, grinding the organization's decision-making processes to a halt.

Delegated management elegantly solves this problem by creating a specialized hierarchy for decision-making. Authority is concentrated in a board of directors and a cadre of professional executives who possess the requisite expertise, industry experience, and, most importantly, the dedicated time to manage the firm's complex affairs. This structure, as described by Kraakman et al. (2017), is a profound economizing force. The board, typically elected by the shareholders, serves a dual function: it actively participates in managing the business and affairs of the company while simultaneously engaging in the critical oversight of the senior executives who handle day-to-day operations. This system, which can be structured as a single-tier board (combining management and supervision) or a two-tier board (formally separating these functions), allows for the kind of agile and informed decision-making that would be utterly unattainable under a model of direct owner control.

While delegation is an effective solution to the problem of scale, it simultaneously creates a new and equally profound challenge: the principal-agent problem. First articulated in the context of the modern firm by A Gardiner Means and later formalized with economic rigor by Michael Jensen and William Meckling, this dilemma arises from the potential divergence of interests between the owners (principals) and the managers (agents) to whom they have delegated control (Jensen & Meckling, 2019; Means, 2017). The shareholders, as the firm's residual claimants, are incentivized to maximize the long-term value of the enterprise. The managers, however, may be driven by different priorities. They might, for example, prioritize short-term revenue targets to maximize their annual bonuses, even at the expense of crucial long-term strategic investments. They might engage in "empire-building", pursuing costly and ultimately value-destroying mergers and acquisitions to increase the size of the company under their control and, by extension, their own prestige and compensation. Or, in a simpler manifestation of this conflict, they might simply shirk their responsibilities, not working as diligently as they would if they were the sole owners of the enterprise (Means, 2017).

This fundamental misalignment of interests gives rise to what economists term "agency costs," which represent the total economic losses resulting from this inherent separation of ownership and control. Jensen and Meckling usefully categorize these costs into three distinct types. First are *monitoring costs*, which are the resources expended by the principals to oversee and control the agents' behavior (Jensen & Meckling, 2019). This includes the costs of establishing and maintaining a board of directors, conducting external financial audits, implementing complex

internal reporting systems, and imposing operational constraints on management. Second are *bonding costs*, which are the costs incurred by the agents themselves to signal their trustworthiness and alignment to the principals. This can include agreeing to complex incentive-based compensation contracts (such as stock options) that are designed to align their financial interests with those of the shareholders, or accepting contractual limitations on their own decision-making power. Finally, there is *residual loss*. This represents the ultimate, unavoidable cost of the agency relationship, the monetary loss resulting from decisions made by agents that do not maximize the value of the firm, even after all monitoring and bonding efforts have been undertaken. The entire edifice of corporate law can be understood as a sophisticated system designed to minimize these collective agency costs.

5.7.2 Corporate Law as a Solution to Agency Costs

The entire edifice of modern corporate law can be understood as a sophisticated and multi-layered system designed precisely to minimize these agency costs and to protect the interests of the shareholder-principals from potential exploitation by their managerial agents. It achieves this through a carefully balanced combination of structural rights, procedural rules, and, most importantly, legally imposed duties that govern the conduct of those in power (Kraakman et al., 2017).

The most powerful of these legal tools are fiduciary duties, which are stringent legal obligations that compel managers and directors to act in the best interests of the corporation and its shareholders. The duty of loyalty requires agents to subordinate their personal interests to those of the corporation, strictly prohibiting activities such as self-dealing, the usurpation of corporate opportunities, and other forms of conflicted transactions where their personal benefit might come at the firm's expense. The duty of care, meanwhile, requires them to act with the diligence, prudence, and informed judgment that a reasonable person in a similar position would exercise under comparable circumstances. These duties are not mere ethical guidelines or aspirational statements; they are legally enforceable obligations that provide a powerful basis for shareholders to bring derivative lawsuits against directors and officers for mismanagement, negligence, or disloyalty, thereby creating a potent deterrent against self-interested behavior (Hacker, 2019).

Beyond these overarching duties, corporate law provides shareholders with a set of direct control mechanisms. Appointment rights grant shareholders the power to elect the board of directors, who serve as their primary representatives within the corporate hierarchy. Decision rights ensure that the most fundamental corporate actions, such as mergers, the sale of substantially all of the company's assets, or amendments to the corporate charter, require the affirmative approval of the shareholders (Kraakman et al., 2017). Finally, extensive mandatory disclosure regimes, which require regular and audited reporting of financial information, serve to reduce the information asymmetry between corporate insiders and the firm's owners, enabling more effective monitoring and holding management accountable for its performance.

5.7.3 An Ideological Break: Eliminating the Agent

The DAO model begins with a radical and uncompromising premise: that the entire trust-based, hierarchical structure of the corporation is an obsolete artifact of a pre-digital age. It posits that the principal-agent problem is not a mere bug to be patched with the legal fixes of corporate law, but rather a fundamental and incurable flaw in the corporate architecture itself. The DAO's proposed solution, therefore, is to dismantle this architecture entirely. It aims to operate without a central locus of control or a formal managerial hierarchy, thereby seeking to eliminate the agent and dissolve the agency problem at its very source (Morrison et al., 2020; Weinstein & Loftchie, 2022).

This ambitious goal is to be achieved by hard-coding the organization's rules into self-executing smart contracts on a blockchain. In this model, the discretion and potential fallibility of human intermediaries are replaced by the rigid and predictable logic of algorithmic execution (Sims, 2019). Decision-making is not delegated to a board of directors; instead, token holders are empowered to propose and directly vote on all organizational matters, from minor operational changes to major strategic shifts (Biyan Mienert, 2024). An approved proposal does not require a CEO's signature or a board resolution to be implemented; the underlying smart contract executes the specified action, be it a transfer of funds from the treasury, a change in a protocol parameter, or the deployment of entirely new code, automatically and, in many cases, irrevocably. This peer-to-peer decision-making process is the technical and philosophical core of the DAO's attempt to re-bundle ownership and control, creating what its proponents hope will be a more transparent, equitable, and perfectly aligned organizational form (Charlton et al., 2023; Wright, 2021).

5.7.4 The New Governance Dilemmas of Direct Democracy

While this vision of direct, automated governance is theoretically elegant, its practical application has revealed a new set of complex challenges that, ironically, often mirror the very problems of power, apathy, and inefficiency that plague traditional corporations. The first and most pervasive of these issues is voter apathy. For the vast majority of token holders in any given DAO, the cost in time and effort required to stay sufficiently informed on a constant stream of often highly technical and financially complex proposals is prohibitively high. This phenomenon, known in political science as "rational ignorance," leads to extremely low voter turnout, as the perceived impact of a single smallholder's vote is negligible when weighed against the significant effort required to cast an informed one (Nunes Teixeira, 2023).

This widespread apathy creates a dangerous power vacuum that is inevitably filled by a small number of large token holders, or "whales", often the venture capital firms that provided initial funding, the project's founders, or other early insiders. With their immense and concentrated voting power, these actors can easily dominate governance outcomes, creating a *de facto* plutocracy or oligarchy that operates under the guise of decentralized democracy (Wright, 2021). This dynamic effectively recreates the separation of ownership and control in a new form: a vast, passive base of small token holders is, in practice, governed by a small, concentrated group of powerful insiders. This outcome directly undermines the core promise of decentralization and reintroduces a new

type of agency problem, but one that exists in a legal vacuum without the traditional protections of fiduciary duty (Nunes Teixeira, 2023; Ziolkowski et al., 2020b).

Second, the process of managing a dynamic and complex enterprise through direct on-chain voting is often untenably slow and operationally inefficient. The formal process of drafting a proposal, subjecting it to public debate within the community, and conducting a multi-day vote is ill-suited for the kind of rapid, agile, and often confidential decision-making that is required to compete effectively in the marketplace or respond to unforeseen crises. This significant operational drag makes it exceptionally difficult for DAOs to react effectively to emerging threats or to seize fleeting opportunities, placing them at a distinct competitive disadvantage relative to their more centralized, corporate counterparts.

5.7.5 The Pragmatic Convergence: The Re-Emergence of Delegation

Faced with these significant functional limitations, a clear evolutionary trend has emerged across the DAO ecosystem: the organic and pragmatic re-introduction of delegation. Mature and sophisticated DAOs are increasingly abandoning the ideological purity of pure direct democracy in favor of more practical, hybrid models that blend the ideal of decentralized oversight with the necessity of specialized, delegated execution. This convergence represents a tacit acknowledgment that while the specific *form* of the corporate board of directors may be an artifact of a pre-digital era, the core *function* of delegation remains a persistent and inescapable necessity for effective organizational management at any significant scale. The challenge for DAOs is not to eliminate delegation, but to reinvent it in a way that is compatible with their decentralized ethos.

This re-emergent delegation manifests in several key structures that are now common across the DAO landscape. Many DAOs now create specialized working groups, sometimes referred to as "pods" or sub-DAOs, which are focused on specific operational areas such as treasury management, marketing and communications, business development, or the administration of grant programs. These groups are often granted a significant degree of autonomy and a designated budget to execute tasks on behalf of the broader DAO, functioning in a manner that is highly analogous to traditional corporate departments (Boss, 2023). To improve agility and overcome the slow pace of on-chain voting for routine matters, some DAOs elect smaller councils or committees to make certain types of decisions or to act as trusted signatories on the multi-signature wallets that control treasury funds. These elected bodies serve a function that is functionally equivalent to a corporate board's executive committee, empowered to act more swiftly and decisively than the entire token holder base could.

In protocol-focused DAOs, the core development teams that initially built and continue to maintain the underlying code are often implicitly or explicitly empowered to manage the technical roadmap and its implementation. In this model, the broader community of token holders provides high-level strategic direction and formal approval for major upgrades, but the specialized work of software development is delegated to a trusted group of experts. Finally, in a direct response to the pervasive problem of voter apathy, many DAOs are implementing advanced systems of vote delegation, often referred to as "liquid democracy." This powerful

mechanism allows individual token holders to entrust their voting power to a trusted expert, community representative, or "protocol politician" who then votes on their behalf (Axelsen et al., 2023). This creates a fluid and dynamic system of representation that begins to closely resemble the shareholder-director relationship, albeit with greater flexibility for token holders to re-delegate or reclaim their votes at any time.

5.7.6 The Legal and Accountability Vacuum

This pragmatic and necessary shift toward hybrid governance models highlights a critical legal and regulatory gap at the heart of the DAO ecosystem. The corporate system of delegated management is backstopped by a robust and centuries-old legal framework centered on the concept of fiduciary duty. Directors and officers are legally accountable for their actions and have a clear, enforceable duty to act with care and loyalty in the best interest of the corporation and its shareholders. In the world of DAOs, this essential legal framework is largely absent.

The delegates in these new, emergent structures, be they working group leaders, elected council members, or core developers, generally operate without the defined legal status or the legally imposed fiduciary duties of their corporate counterparts (Hacker, 2019). The prevailing ethos of "code is law" provides a technical and procedural logic for governance but does not, and cannot, adequately cover the vast range of situations that require human judgment, good faith, prudence, or undivided loyalty, particularly in unforeseen or ambiguous circumstances (Nunes Teixeira, 2023).

This absence of a legal framework for accountability creates a crisis. When a DAO's treasury is mismanaged by a delegated committee, or when a core team makes a disastrous strategic error, who is legally responsible? The lack of a formal board structure or identifiable officers makes it exceedingly difficult for both internal participants and external regulators to assign liability and seek recourse (Schillig, 2022). This legal ambiguity poses a major risk to the entire system. In the absence of a clear corporate form that defines the roles and responsibilities of these new delegates, courts and regulators are more likely to fall back on the default classification of a general partnership, a move that would impose joint and several liability on all participating members, thereby punishing the entire community for the potential failings of a few delegated actors (Florian Möslein & Daniel Ostrovski, 2024; Sims, 2019).

Recognizing this peril, new DAO-specific legislation, such as the LLC laws in Wyoming and Utah, attempts to bridge this gap by providing a liability shield. However, these laws often do so by requiring the designation of administrators or official representatives, effectively re-imposing a centralized point of legal accountability that can blur the line between the decentralized ideal and the traditional corporate form (Boss, 2023).

5.7.7 Conclusion on the Management

The principle of delegated management reveals a fundamental and enduring tension between organizational ideals and operational realities. The traditional corporation embraces a hierarchical model of delegation that, while highly efficient, introduces the persistent conflict of the principal-agent problem, which centuries of corporate law have been developed to contain. The DAO, in its purest ideological form, seeks to obliterate this hierarchy entirely through a system of direct, code-enforced governance. Yet, in doing so, it confronts intractable challenges of scale, efficiency, and voter apathy that ultimately force it to organically reinvent delegation in new, legally ambiguous forms.

The trajectory of the DAO from a purely flat, decentralized ideal toward a more pragmatic, hybrid structure demonstrates that the *function* of delegation, the empowering of smaller, specialized groups to act on behalf of the whole, is an enduring and likely indispensable feature of successful large-scale human coordination. What is radically changing is the *form* this delegation takes and the legal framework that governs it. This fundamental re-imagining of management and control leads directly to the next and final core attribute of the firm: the nature of ownership itself. How the rights to control an organization are structured, whether through the indirect representation of the corporate model or the direct participation of the DAO model, profoundly shapes what it means to be an owner. We now turn to an analysis of investor ownership, exploring how the shift from the corporate shareholder to the DAO token holder redefines the rights, risks, and responsibilities associated with providing capital to a collective enterprise.

5.8 Investor Ownership: From Residual Claimants to Participant Governors

The final, and arguably most defining, attribute of the modern business enterprise is the principle of investor ownership. This concept addresses the fundamental question at the heart of any collective enterprise: for whom is the firm managed, and to whom do its ultimate successes and failures belong? In the traditional corporate paradigm, the answer to this question is unequivocal: the firm is owned by, and operated for the primary benefit of, its shareholders, the providers of equity capital who bear the enterprise's ultimate financial risk (Kraakman et al., 2017). This model, which vests both the ultimate rights to control the firm and the rights to its net profits (its residual claims) in its capital investors, has proven to be an extraordinarily effective engine for aggregating the vast sums of capital necessary to fuel the global economy (Hansmann, 2000). The entire legal architecture of the corporation, meticulously constructed upon the pillars of legal personality, limited liability, transferable shares, and delegated management, is designed to support and facilitate this specific model of investor ownership. In this framework, the shareholder stands at the apex of the corporate structure, not as a day-to-day manager, but as the ultimate beneficiary and final arbiter of the firm's direction, exercising power indirectly through their elected representatives on the board of directors.

The Decentralized Autonomous Organization presents a profound and disruptive challenge to this long-standing and deeply entrenched model. It seeks to deconstruct and radically reconfigure the very meaning of "ownership" in a collective enterprise. By leveraging the unique affordances of

blockchain technology, the DAO blurs the traditionally clear and legally demarcated roles of investor, manager, user, and employee, often merging them into a single, multifaceted identity: the token holder (Hassan & De Filippi, 2021). In a DAO, ownership is no longer a legally defined status granting indirect control and a formal claim on profits, but rather a technologically-defined and enforced right to direct participation in the organization's governance. This section explores this fundamental divergence in the nature of ownership. First, it will delve into the corporate paradigm, explaining the powerful economic rationale for the primacy of the shareholder as the firm's residual claimant and the indirect nature of their control. It will then contrast this with the DAO's novel model of participatory governance, where token holders act as a fusion of owner, governor, and user, and where their economic rights are often ambiguous and uncoded.

5.8.1 The Corporate Paradigm: The Primacy of the Shareholder as Residual Claimant

The global dominance of investor ownership is not an accident of history but the product of a powerful and compelling economic logic. As articulated by legal and economic theorists like Henry Hansmann, the most efficient group to entrust with the ultimate control of a firm is typically the one whose interests are best aligned with maximizing the firm's total value while minimizing the costs of collective decision-making (Hansmann, 2000). In most large-scale business enterprises, that group is the equity investors.

The key to this alignment lies in their unique status as the firm's residual claimants. Shareholders are entitled to the profits of the enterprise only after all other parties with fixed, contractual claims, including employees owed wages, suppliers owed payments, and creditors owed interest and principal, have been paid in full (Kraakman et al., 2017). In the event of a liquidation, they are the very last in line to claim any of the company's remaining assets. This precarious financial position is precisely what makes them, in theory, the most effective stewards of the firm. Because their returns are entirely dependent on the value that remains after all other costs have been met, their singular and overriding incentive is to ensure the firm is managed in a way that maximizes that residual value. This creates a powerful alignment between the owners' financial interests and the long-term health and profitability of the corporation as a whole. Furthermore, when compared to other potential stakeholder groups, such as employees or customers, shareholders tend to have relatively homogenous interests, namely, the maximization of financial returns. This shared objective significantly reduces the potential for costly internal conflicts and simplifies the process of collective decision-making, even when that decision-making is delegated to a board of directors (Armour et al., 2017).

In corporate law, ownership is not an abstract concept but a legally defined "bundle of rights" that is embodied in the corporate share (J. G. Allen, 2020). This bundle primarily consists of two distinct components: economic rights and control rights. The core economic right of a shareholder is the legal claim to a pro-rata share of the corporation's residual earnings. This claim is typically realized in one of two forms. Dividends represent discretionary distributions of the firm's current or retained earnings to its shareholders, while capital appreciation reflects the increase in the market value of the shares themselves, which investors can realize by selling them on a secondary

market (Weinstein & Loftchie, 2022). This legally enforceable right to the firm's residual earnings is the fundamental reward for providing risk capital to the enterprise.

While shareholders are the ultimate owners, their control is, in almost all large corporations, indirect. In a publicly held corporation, the widely dispersed and often passive shareholder base is effectively "powerless" to manage the firm directly (Kraakman et al., 2017). Instead, their control is exercised through a limited but crucial set of voting rights. Primarily, they vote to elect the board of directors, who then act as their fiduciaries and are tasked with overseeing the professional managers who run the company on a day-to-day basis (Easterbrook & Fischel, 1996). They also typically vote on the most fundamental corporate changes, such as mergers, the sale of the company, or significant amendments to the corporate charter (Armour et al., 2009). This model of indirect control is a direct and necessary consequence of the principle of delegated management, which allows ownership to be separated from the specialized function of daily operations. The viability and attractiveness of this entire ownership model are completely dependent on the other four corporate attributes. Legal personality ensures the firm can own assets separately from its owners. Limited liability protects the shareholders' personal assets, capping their risk to the amount of their investment and thereby encouraging diversification (Armour et al., 2009). Finally, transferable shares provide the liquidity that allows investors to easily enter and exit their positions, forming the very basis for modern capital markets. Together, these attributes create the robust, predictable, and risk-mitigated framework that has made shareholder ownership the dominant model for capital formation across the globe.

5.8.2 The Blurring of Roles: The Token Holder as a Hybrid Actor

The DAO fundamentally reimagines the concept of ownership by collapsing the distinct and carefully separated roles that characterize the traditional corporation. Where the corporate model meticulously distinguishes the shareholder (owner) from the manager (agent), the employee (labor), and the customer (user), the DAO often merges these functions into the single, multifaceted role of the token holder. Ownership in a DAO is established not through a legally registered share certificate, but through the cryptographic possession of network tokens (Borgogno & Martino, 2024). A single token can grant its holder a dynamic and programmable bundle of rights that transforms them into a hybrid actor within the organization's ecosystem. A token holder is simultaneously: an *investor*, acquiring tokens with the expectation that their value will appreciate as the DAO's protocol or treasury grows (Weinstein & Loftchie, 2022); a *governor*, using the token to vote directly on a wide spectrum of operational and strategic proposals, effectively participating in management (Armour et al., 2009); a *user*, as the token may be required to access the services or platform that the DAO provides; and, in many cases, a *worker*, as participants can contribute labor in areas like software development or community management and receive token-based rewards in return.

This fusion of roles is a core feature of the DAO ethos. From the perspective of transaction cost economics, which posits that firms exist to minimize the costs of coordination (Williamson, 1981), the DAO represents a radical experiment. It utilizes blockchain as a new institutional technology to drastically reduce the costs associated with direct collective action, making it possible for

thousands of participants to govern an organization directly in a way that was previously unimaginable in the pre-digital world (Beck et al., 2018).

5.8.3 The Nature of Token Ownership: Direct Control and Ambiguous Claims

The "bundle of rights" represented by a DAO token is fundamentally different from that of a corporate share, particularly in its profound emphasis on direct control and the corresponding ambiguity of its economic claims. Unlike the indirect, representative control of a corporate shareholder, the token holder is empowered with direct and immediate involvement in governance. Token-based voting, typically on a "one-token, one-vote" basis, allows participants to decide on everything from minor protocol upgrades and treasury allocations to major strategic pivots and hiring decisions (Peder Østbye, 2024; World Economic Forum, 2022). This mechanism aims to instantiate a form of direct digital democracy, collapsing the distance between owners and the organization itself in an attempt to eliminate the agency costs associated with delegation (De Filippi & Wright, 2018).

Herein lies the most critical legal divergence from the corporate model: the nature of the economic rights. While DAO tokens can and do appreciate in value, they typically do not grant their holders a legally enforceable claim to a share of the organization's profits or assets. The concept of a dividend-like distribution is rare, and more importantly, the legal status of a token holder as a residual claimant is entirely undefined in most jurisdictions. In the event of a DAO's dissolution or failure, there is often no clear legal or even code-based process for distributing the remaining treasury assets to the token holders. This leaves them in an extremely precarious legal position, lacking the fundamental creditor-like protections that are afforded to traditional shareholders in a liquidation scenario.

5.8.4 The Legal and Practical Ambiguities of DAO Ownership

The DAO's innovative approach to ownership, while powerful in its participatory promise, creates a host of profound legal and practical challenges that stem from its fundamental clash with existing legal frameworks. First, the model of direct governance, while aiming for decentralization, is highly susceptible to plutocratic capture. As discussed previously, widespread voter apathy often means that governance is dominated by a few "whales" with large token holdings (Barbereau et al., 2022; Ziolkowski et al., 2020a). This creates a new and potent power imbalance, but one that operates in a legal vacuum. In a corporation, the board of directors owes legally enforceable fiduciary duties to the corporation that serve to protect minority shareholders from exploitation by a controlling majority. In a DAO, these duties are generally absent, meaning a 51% coalition of token holders could potentially vote to alter the protocol in a way that benefits them at the direct expense of the minority, with far fewer legal repercussions or avenues for recourse (Nunes Teixeira, 2023).

Second, the very legal status of the DAO owner is dangerously uncertain. As established in the sections on legal personality and limited liability, a DAO that fails to adopt a formal legal "wrapper" is likely to be treated by default as a general partnership (Weinstein & Loftchie, 2022). This legal alchemy transforms the token holder from a passive investor with limited liability into a general partner with unlimited, joint, and several personal liability for all of the DAO's debts and obligations (Sims, 2019). This represents a catastrophic risk profile that is fundamentally incompatible with the goal of attracting widespread, mainstream investment and participation. The unique sociotechnical features of DAOs, their fluid, transnational memberships, pseudonymous contributions, and governance over open-source protocols, are "testing the boundaries of legal orders" (De Filippi et al., 2022). Existing legal entity types were not designed for such structures, making it difficult for legal systems to classify DAOs and their tokens, thereby leaving their owners in a state of profound and untenable legal uncertainty (J. Z. Tan et al., 2023).

5.9 Conclusion of the Comparative Analysis

The journey through the five core attributes of the modern enterprise reveals the DAO as both a powerful evolution in organizational technology and a profound challenge to the very foundations of commercial law. The traditional corporation is an elegant, legally-sophisticated construct designed to support a specific model of investor ownership, made possible by the interlocking pillars of legal personality, limited liability, transferable shares, and delegated management. This framework provides the certainty, predictability, and risk mitigation necessary to attract and deploy capital at a global scale.

The DAO disrupts every one of these pillars. It struggles to achieve legal personality and limited liability, exposing its participants to the archaic and severe risks of partnership law. It supercharges the concept of transferability through tokens but runs headlong into a century-old securities law framework that it was not designed for. It attempts to eliminate delegated management in favor of direct democracy but finds itself grappling with inefficiency and organically reinventing delegation without the essential legal safeguards of fiduciary duty. And finally, as we have seen in this section, it deconstructs the very concept of investor ownership. It replaces the legally-defined residual claimant with a multi-faceted participant-governor, trading the clear, enforceable economic rights of the shareholder for the promise of direct, programmatic control.

While this new paradigm of participatory ownership offers a compelling vision for a more transparent and aligned future of collective enterprise, its long-term viability remains an open question. Until a new, bespoke legal and regulatory framework emerges that can provide clarity and protection for this novel form of organization, the DAO will remain a powerful but precarious experiment, caught between its technologically-advanced architecture and a legal world that is still struggling to comprehend it. The following sections will explore in greater detail the current attempts by regulators in the United States and the European Union to bridge this gap, before concluding with a proposed blueprint for a more coherent path forward.

5.10 Regulatory Landscape for DAOs in the European Union and the United States

As explained in the previous sections, the exponential growth of Decentralized Autonomous Organizations (DAOs) and the challenges and risks it bring have triggered an urgent need for legal recognition and regulatory adaptation in major jurisdictions. While DAOs represent an unprecedented experiment in algorithmic governance and collective decision-making, their interaction with law remains uncertain and challenging. Legal systems built upon the assumptions of centralization, identifiable management, and territorial jurisdiction struggle to accommodate entities that are borderless, pseudonymous, and governed by code (De Filippi & Wright, 2018). As of 2025, both the European Union (EU) and the United States (US) have adopted piecemeal and often conflicting approaches. The EU follows a cautious, “*wait-and-see*” strategy, relying on existing corporate and financial regulations while studying blockchain phenomena through policy experimentation. The US, conversely, demonstrates a dual-level system: *fragmented federal enforcement* coexists with *state-level innovation*, where a handful of jurisdictions have attempted to legally recognize DAOs through bespoke statutes.

Despite their different legal traditions, the EU’s supranational law structure and the US’s federal law framework, both regions share a common dilemma: DAOs disrupt the foundational premises of law, such as legal personality and accountability. Moreover, without a recognized legal form, DAOs risk being treated as unincorporated associations or general partnerships, exposing participants to unlimited personal liability (Weinstein & Loftchie, 2022). Regulatory responses, therefore, oscillate between enforcing existing norms and crafting experimental solutions that reconcile technological autonomy with legal responsibility.

5.10.1 Federal-Level Approaches in the US

At the federal level, US regulators have primarily applied *legacy financial statutes* to DAOs, often through enforcement rather than legislative innovation. The *Securities and Exchange Commission (SEC)*, *Commodity Futures Trading Commission (CFTC)*, *Internal Revenue Service (IRS)*, and *Office of Foreign Assets Control (OFAC)* have each extended their authority to decentralized systems, producing overlapping jurisdictions and regulatory uncertainty (Brook Knight, 2017; Weinstein & Loftchie, 2022).

5.10.1.1 a. The SEC and the Securities Paradigm

The SEC’s 2017 Report on “The DAO” marked a turning point. It concluded that DAO tokens constituted securities under the *Howey test*²⁰, establishing that even decentralized offerings could fall under securities regulation if investors expected profits derived from others’ efforts

²⁰ The *Howey test*, derived from *SEC v. W.J. Howey Co.* (1946), determines whether a transaction constitutes an “investment contract,” and therefore a security, under U.S. law. The test asks whether there is (1) an investment of

(Securities and Exchange Commission, 2017). This interpretation set a precedent: decentralization does not negate securities law applicability. However, it also imported the rigid categories of mid-20th-century jurisprudence, such as *the Howey test*, into a context where roles are fluid, token holders may simultaneously act as investors, governors, and contributors (Schwiderowski et al., 2024).

The Commission's continued reliance on enforcement has drawn criticism for fostering "regulation by litigation" (Blemus, 2023). Lacking formal rulemaking, projects remain uncertain whether they qualify as securities until after the fact. In response, *Commissioner Hester Peirce's Safe Harbor proposal* suggested a three-year grace period for token networks to achieve sufficient decentralization before facing registration requirements (Hester M. Peirce, 2021). While never adopted, this framework reflects growing awareness that innovation requires adaptive legal thresholds.

5.10.1.2b. The CFTC and Commodity Oversight

The CFTC's landmark case *CFTC v. Ooki DAO (2022)* confirmed that a DAO could be treated as an "unincorporated association," holding governance participants personally liable for violations of the Commodity Exchange Act (Commodity Futures Trading Commission, 2022a; Vandy, 2024). This decision extended joint and several liability principles into decentralized governance, meaning a simple governance vote could trigger personal accountability. The chilling effect on community participation was immediate and profound. Moreover, the case intensified interagency friction: the SEC classifies many DAO tokens as securities, while the CFTC regards them as commodities, leaving developers navigating an "alphabet soup" of regulators with overlapping mandates (Weinstein & Loftchie, 2022).

5.10.1.3c. Taxation and Sanctions

The IRS further complicates matters by classifying cryptocurrencies as "property" rather than currency, creating onerous reporting obligations for DAO participants who may lack identifiable tax jurisdictions (Dimitropoulos, 2020). Simultaneously, *OFAC's 2022 sanction of Tornado Cash*, a privacy protocol governed in part by a DAO, demonstrated the government's willingness to treat code itself as a sanctionable entity (U.S. Department of Treasury, 2022). The constitutional implications are profound: sanctioning immutable smart contracts challenges the distinction between technology and human agency (*Bernstein v. U.S. Department of Justice*, 1999).

5.10.1.4d. Legislative Proposals and Inertia

money (2) in a common enterprise (3) with an expectation of profits (4) derived predominantly from the efforts of others. If all four prongs are satisfied, the arrangement falls under federal securities regulation.

Despite numerous congressional proposals, including the *Responsible Financial Innovation Act* and the *Lummis-Gillibrand Act*, no federal statute specifically governing DAOs has been enacted (Weinstein & Loftchie, 2022). These bills typically propose registration as LLCs or corporate entities, yet such frameworks fail to capture the fluidity and decentralization of DAO governance (Vandy, 2024). Consequently, DAOs remain in a regulatory limbo where compliance is theoretically expected but practically unattainable.

5.10.2 State-Level Innovations from the US: Laboratories of DAO Law

The United States' subnational jurisdictions have become fertile laboratories for experimenting with legal personhood in the decentralized economy. While federal inaction continues to produce a vacuum of legal certainty, state legislatures, most notably Wyoming, Utah, Vermont, and Tennessee, have stepped forward to develop bespoke DAO statutes. These initiatives, motivated by the same “regulatory competition” dynamics that shaped twentieth-century corporate law, illustrate an evolving effort to adapt the limited liability company (LLC) model to blockchain-based organizations (Weinstein & Loftchie, 2022). Together, they represent an early attempt to integrate *code-based governance* into the language of positive law.

5.10.2.1 a. Wyoming: The DAO LLC

Wyoming's 2021 Decentralized Autonomous Organization Supplement to its LLC Act marks the first codified recognition of DAOs in U.S. law. It permits registration of DAOs as “DAO LLCs”, which may be *member-managed* or *algorithmically managed* entities (Wyo. Stat. §17-31-106, 2021). This statute goes beyond symbolic recognition by embedding blockchain logic into state corporate law: it explicitly accepts smart contracts as governing instruments, thereby translating the principle of “code is law” into statutory form. In doing so, Wyoming provides DAOs with the capacity to own assets, contract, sue, and be sued, and crucially, grants limited liability to members.

However, the statute's minimalist approach has drawn critique. It waives traditional fiduciary duties unless expressly included in the operating agreement, an omission that may leave tokenholders without recourse for managerial abuse or negligence (Boss, 2023). Empirical findings suggest that DAO participants value legal clarity not merely for formality, but for the sense of trust and legitimacy it provides (Boss, 2023). The Wyoming framework delivers formal certainty but neglects the substantive governance safeguards that support sustainable decentralization. Moreover, the territorial nature of state law constrains its extraterritorial recognition: a DAO LLC registered in Wyoming may still be treated as an unincorporated association in another jurisdiction, leaving members exposed to liability. This conflict-of-laws highlights the fragility of national innovation within a transnational system (Finck, 2018).

5.10.2.2b. Utah and Vermont: Expanding the Model

Other states have refined Wyoming's template by adding elements of transparency, consumer protection, and technical accountability. The Utah DAO Act (2023) introduces the Limited Liability DAO (LLD), which requires registration, public disclosure of the DAO's smart-contract address, and code auditing prior to recognition (Boss, 2023). This design borrows heavily from the COALA Model Law for DAOs, a non-binding international framework proposing entity status for DAOs that meet openness and governance criteria. By grounding its provisions in this model, Utah's statute embodies a "future-proof" approach, flexible enough to accommodate technological evolution while safeguarding participants.

Vermont, in contrast, adopts a hybrid corporate approach through its Blockchain-Based Limited Liability Company (BLLC) statute (2018). The BLLC recognizes both algorithmic and human-managed systems, explicitly permitting DAOs to coexist with off-chain governance (Weinstein & Loftchie, 2022). Empirical studies show that many DAOs prefer such dual structures, using the on-chain layer for transparency and coordination while maintaining traditional legal representation off-chain for contracting and tax purposes (Boss, 2023). Vermont's model, though conservative, acknowledges this operational hybridity and reflects a pragmatic reconciliation of innovation with administrative feasibility.

5.10.2.3c. The Jurisdictional Fragmentation

Despite their ambition, these state statutes collectively expose a persistent jurisdictional fragmentation problem. Law is territorially bound, whereas DAOs are borderless networks. A Wyoming or Utah DAO might host nodes across Europe, Asia, and South America, yet its limited liability protection may evaporate once foreign law applies. Most DAOs still face "legal invisibility" in jurisdictions that lack explicit recognition, resulting in default classification as general partnerships with unlimited liability (Weinstein & Loftchie, 2022). The risk is amplified by the DAO's pseudonymous membership and cross-border activity, which complicates both enforcement and taxation.

Empirical evidence further reveals that DAO communities are aware of this legal vacuum. Respondents in Boss's (2023) survey identified limited liability, tax clarity, and dispute resolution as their top legislative priorities, emphasizing that the absence of international harmonization undermines not only participation but also governance legitimacy (Boss, 2023). Until mutual recognition frameworks emerge, perhaps building on the COALA Model Law or OECD-style soft-law cooperation, state-level innovation remains a partial solution. It grants local certainty but fails to resolve global exposure. DAOs inhabit a "post-territorial legal paradox": they require jurisdictional anchoring to achieve legitimacy, yet that very anchoring fragments their decentralized essence (Boss, 2023).

5.10.2.4d. Centralization Problem

Moreover, the very statutory frameworks designed to legitimize DAOs paradoxically reintroduce elements of *centralization* that undermine their decentralized ethos. State laws such as those of *Wyoming* and *Vermont*, though intended to confer legal personality and limited liability, impose mandatory requirements that conflict with the foundational principles of distributed governance. Under *Vermont's Blockchain-Based Limited Liability Company (BLLC)* legislation, every entity must appoint a *registered agent* and maintain a *designated office* for notification purposes. These requirements establish a physical point of contact and a legally responsible intermediary, both of which are antithetical to the notion of a borderless and self-governing digital organization (Perestrelo de Oliveira & Rolo, 2024). Similarly, *Wyoming's DAO LLC* statute, while permitting algorithmic or member-based management, still mandates the appointment of a state-registered agent. Although this agent need not act as a manager, their existence embeds a *central node of accountability* within the DAO's legal architecture, creating a hybrid form that sits uneasily between automation and representation (Perestrelo de Oliveira & Rolo, 2024).

From this perspective, the process of “*wrapping*” a DAO within an LLC or similar legal entity inherently introduces *centralizing vectors*, including compliance with corporate governance norms such as maintaining a registered office, submitting filings, and identifying human representatives. These requirements generate a “*compliance-induced centralization*,” in which legal obligations force decentralized communities to designate individuals or small groups to interact with the legal system on their behalf (Boss, 2023). While these intermediaries facilitate access to limited liability and recognition before the law, they simultaneously reintroduce the very hierarchical and personified features DAOs were designed to transcend. Therefore, DAO-LLC statutes, despite their innovative intent, retain traditional LLC structures such as fixed articles of organization, amendment procedures, and membership registers (Boss, 2023). These *static governance mechanisms* are incompatible with the *fluid, code-based, and evolving membership* that characterizes most DAOs, thereby constraining their flexibility and autonomy.

This tension produces an unintended contradiction: in order to gain legal protection, DAOs must partially *abandon their decentralization*, adopting institutional attributes of the corporate entities they sought to replace. Legal wrappers thus function as *double-edged tools*, they safeguard participants through liability shields while simultaneously embedding bureaucratic and centralized features that erode algorithmic autonomy (Boss, 2023; Perestrelo de Oliveira & Rolo, 2024). As a result, while LLC-based DAO statutes provide a bridge between code and law, they also reveal a deeper structural dilemma: *law can only recognize decentralization by recentralizing it* through representation, registration, and accountability mechanisms.

5.10.3 The European Union: A Cautious Integration Approach

In contrast to the US's enforcement-driven model, the EU has adopted a *principle-based, cautious regulatory philosophy*, embedding DAOs within its broader digital asset and financial market strategies rather than legislating standalone DAO laws. The European Commission has repeatedly

emphasized a “*technological neutrality*”²¹ stance, ensuring that existing legal norms apply regardless of the underlying technology (European Commission, 2022). As a result, DAOs currently fall under the indirect purview of instruments like the *Markets in Crypto-Assets Regulation (MiCA)*, the *Digital Finance Package*, and the *DORA Regulation* on operational resilience.

This cautious integration reflects both legal and political pragmatism. The EU’s civil law tradition prioritizes codified, harmonized frameworks over the ad hoc adaptation characteristic of common law systems. However, it also leaves significant ambiguity: while *MiCA* establishes comprehensive rules for crypto-asset issuers and service providers, it does not explicitly address DAO governance or decentralized corporate forms (Boss, 2023).

5.10.3.1 DAOs and MiCA: Partial Coverage, Persistent Gaps

The *MiCA Regulation (EU 2023/1114)*, entering into force in 2024, constitutes the EU’s flagship effort to regulate digital assets. It classifies crypto-assets into categories, asset-referenced tokens, e-money tokens, and utility tokens, and imposes licensing requirements on issuers and service providers. However, *MiCA*’s scope presupposes the existence of a legally identifiable issuer or service provider, effectively excluding fully decentralized entities.

This omission reflects a structural bias: EU financial regulation is designed around centralized accountability, whereas DAOs disperse control across pseudonymous actors (Schwiderowski et al., 2024). Consequently, DAO-governed protocols offering tokenized financial services risk being treated as *unregulated collective investment schemes* or *even unauthorized market operators*, depending on national transpositions. The result is a regulatory grey zone where DAO participants may incur liability without the protections of formal recognition (Zetsche et al., 2018).

5.10.3.2 Data Protection, Civil Liability and Fragmentation

Beyond financial regulation, DAOs implicate broader EU legal domains. The *General Data Protection Regulation (GDPR)* introduces paradoxes for decentralized systems, particularly concerning data controllership and erasure rights (J. G. Allen, 2020). A DAO storing user data on an immutable ledger faces inherent conflict with the “right to be forgotten.” Likewise, under the *AI Act* and *Digital Services Act*, DAOs engaging in automated decision-making or content moderation may fall within compliance obligations designed for corporate intermediaries. Yet, with no centralized controller, compliance becomes conceptually incoherent (Nunes Teixeira, 2023).

²¹ see, European Commission on *technology neutrality*, <https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elap/technology-neutrality>

Civil liability frameworks are equally unsettled. Under existing directives, responsibility typically attaches to identifiable persons, manufacturers, controllers, or service providers. The DAO's distributed architecture diffuses agency, making it difficult to assign fault or enforce remedies. Some scholars propose adapting collective liability models or creating "*network personhood*" concepts that attribute limited legal standing to decentralized systems (Florian Möslein & Daniel Ostrovski, 2024), but such proposals remain theoretical.

Fragmentation within the European Union further complicates the regulatory landscape. In the absence of DAO-specific legislation, these entities remain subject to *divergent national frameworks*, exposing participants to inconsistent and overlapping obligations across Member States. A DAO operating transnationally may simultaneously trigger the application of financial, consumer protection, and liability laws from multiple jurisdictions, producing significant regulatory uncertainty. This lack of harmonization undermines both innovation and enforcement, as *unregulated domains such as DAOs* become subject to a patchwork of national interpretations and administrative practices.

5.10.3.3 National and Transnational Initiatives

At the national level, *Switzerland* (though outside the EU) remains Europe's most popular jurisdiction for DAOs, offering foundation-based wrappers under the Swiss Civil Code that enable DAOs to obtain limited liability and contractual capacity (Riva, 2021). Within the EU, *Malta's Virtual Financial Assets Act (VFAA)* provides an early model for recognizing "technological arrangements," including DAOs, as entities capable of registration and supervision (Ganado, 2023). *Germany* and *France*, by contrast, have focused on securities tokenization and AML compliance rather than decentralized governance per se.

At the supranational level, the *European Blockchain Services Infrastructure (EBSI)* and the *Blockchain Observatory and Forum* are conducting policy research into decentralized governance models, signaling gradual movement toward institutional recognition. However, without explicit legislation, DAOs remain subject to the same corporate default rules, typically partnerships or associations, rendering their members personally liable for debts and legal breaches (World Economic Forum, 2022).

5.10.4 Comparative Reflections: Convergence and Divergence

The US and EU represent contrasting regulatory philosophies shaped by their institutional architectures. The *US approach* is characterized by vigorous enforcement at the federal level paired with innovative experimentation at the state level. The *EU approach*, conversely, is embedding blockchain governance into existing regulatory ecosystems. Both systems exhibit a gap between the *technological reality of decentralization* and the *regulatory protection*.

Convergence arises in two areas. First, both jurisdictions recognize the necessity of *limited liability* as a precondition for DAO legitimacy, whether through legal wrappers, foundations, or bespoke statutes (Brummer & Seira, 2022). Second, both increasingly view transparency and auditability, core blockchain attributes, as regulatory virtues aligning with public policy goals of trust and accountability (Boss, 2023).

Divergence, however, remains pronounced in implementation. US states have adopted *bottom-up experimentation*, while the EU prefers *top-down harmonization*. The American model fosters innovation but risks legal inconsistency and jurisdictional conflict. The European model ensures coherence but may stifle agility, as supranational lawmaking proceeds slowly and cautiously.

5.10.4.1 *Toward a Harmonized Regulatory Blueprint*

Both regions illustrate that the *core legal problem of DAOs is not technological but institutional*. The challenge is designing a form of legal personhood compatible with decentralization, one that enables accountability without re-centralizing control. Several potential pathways are emerging.

Hybrid structures that integrate on-chain governance with off-chain legal entities, such as *the DAO LLC or Swiss Foundation model*, offer a transitional solution (World Economic Forum, 2022). These “Legal Wrapper 2.0” models can be refined through clearer articulation of the relationship between token-holder votes and directors’ fiduciary duties, thereby preserving decentralization while ensuring enforceability.

Initiatives like the *COALA Model Law for DAOs* propose harmonized principles for global recognition, including minimum transparency standards, open-source governance documentation, and automatic conferral of limited liability upon compliance (Boss, 2023). The model could serve as a template for both EU and US adaptation, mitigating the jurisdictional patchwork that currently plagues the field.

Finally, a transition toward functional and risk-based regulation, where DAOs are assessed according to the nature and impact of their economic activity rather than their technological architecture, offers a pragmatic path to reconciling innovation with legal certainty. In this respect, *the EU Blockchain Regulatory Sandbox* and *the U.S. “Safe Harbor”* initiatives are particularly valuable, as they calibrate regulatory obligations to the systemic risk and societal significance of a given activity rather than to the technology underpinning it. By emphasizing proportionality and functional assessment, these experimental frameworks exemplify a shift from form-based to risk-based governance, enabling innovation to proceed under conditions of accountability and measured oversight.

5.10.5 Conclusion

The regulatory trajectories of the United States and the European Union converge on a common recognition: DAOs cannot remain in a legal vacuum. Yet, their efforts diverge in tempo and philosophy. The US approach, dynamic but fragmented, illustrates the vitality of sub-national experimentation but suffers from inconsistency and enforcement overreach. The EU's cautious integration provides conceptual coherence but leaves DAOs functionally unrecognized. Both frameworks reveal that *the fundamental question is not whether DAOs should be regulated, but how law can evolve without erasing their decentralizing essence.*

The future of DAO regulation will hinge on international cooperation and the gradual emergence of hybrid legal architectures, structures that can reconcile algorithmic governance with human accountability. As these experiments mature, the DAO may become not an outlier but a laboratory for reimagining the very foundations of corporate and administrative law in the digital age.

6 Conclusion and Recommendations

This thesis has conducted a critical and systematic investigation into the profound conceptual and practical collisions that occur when blockchain technology, a system conceived in a techno-libertarian ideology of radical decentralization, confronts the established, centralized, and human-centric frameworks of public and corporate governance. The overarching research question has been to determine how, if at all, a technology designed for algorithmic immutability, programmatic automation, and trustless interaction can be reconciled with legal and institutional systems that are foundationally predicated on human discretion, legal contestability, hierarchical accountability, and state-sanctioned sovereignty. The central argument advanced throughout this work, built upon a synthetic analysis of the technology's ideological origins, its collision with public law, its operationalization in private governance, and its confrontation with corporate law, is that blockchain's revolutionary promise has been decisively neutralized by the normative and structural power of established legal and institutional order. The integration of blockchain is not a story of disruption, but one of cautious institutional adaptation and pragmatic co-option.

This conclusion is twofold. First, in the public sphere, the constitutional state has proven to be a non-negotiable framework. It has systematically stripped the technology of its radical, permissionless nature and "domesticated" it into a permissioned tool that reinforces, rather than subverts, state authority. Second, in the private sphere, the attempt to create a "pure" form of decentralized governance via Decentralized Autonomous Organizations (DAOs) has resulted in a "Legal Misfit" of catastrophic proportions. This experiment has failed to escape the iron laws of organizational economics, leading to an inevitable re-centralization of power, while simultaneously exposing its participants to the most primitive and punitive forms of personal liability, a legal status far worse than the corporate structures it sought to replace. The "rule of law," with its deep roots in human sovereignty and discretion, has, in all instances, proven its supremacy over the rigid, algorithmic absolutism of "code is law."

6.1 Synthesis of Key Findings

This overarching conclusion is the culmination of the evidence and analysis developed sequentially across the four main chapters of the thesis. Each chapter's findings serve as a necessary building block for this final synthesis, tracing blockchain's journey from a revolutionary political proposal to its domestication as a contested institutional tool. The first chapter established the essential philosophical and historical baseline, identifying blockchain technology, epitomized by Bitcoin, not as a neutral database but as a *political and ideological project*. Born from the cypherpunk and techno-libertarian critiques of the 1990s, its primary purpose was to solve a *political* problem: the perceived failure and untrustworthiness of centralized human intermediaries like states, banks, and corporations. The goal was to replace fallible trust in these institutions with *cryptographic certainty*, leading to the ethos of *Lex Cryptographia* or "Code is Law", the belief that rules could be immutably encoded and automatically enforced by a distributed

network, creating a self-sovereign system free from human interference. This revolutionary vision served as the benchmark against which the technology's real-world encounters were measured.

The second chapter performed the *first* test, analyzing the collision between this ideology and the constitutional state. The central finding was the identification of a deep and irreconcilable "Governance Paradox." This paradox reveals that blockchain's most celebrated features function as critical *bugs* within a public law system. Primarily, the rule of law demands dynamic capacity for correction, contestability, and discretionary justice (equity), which is fundamentally incompatible with the absolute, permanent nature of an immutable ledger. Rights like the GDPR's *right to erasure* highlight this clash. Secondly, public law requires clear hierarchical accountability, whereas decentralization intentionally diffuses responsibility, creating an architecture for *impunity* in the eyes of the state. The state's response, evidenced empirically, has been to *reject* this ideology by exclusively preferring private, permissioned blockchains. This represents a domestication and co-option, using the technology to *reinforce* state authority through enhanced auditability and data integrity (e.g., land registries) under central control, rather than to abdicate it.

The third chapter conducted the *second* test, examining Decentralized Autonomous Organizations (DAOs) as the purest experiment in private governance based on the "Code is Law" ideal. The central finding is that this experiment has largely failed on its own terms, inevitably re-centralizing power in new, less accountable forms. Two of the key "governance pathologies" define this failure: the rise of *plutocracy*, where widespread voter apathy allows wealthy "whales" to dominate "one-token, one-vote" systems, and the emergence of a *technocratic elite*, where the complexity of the code grants *de facto* power to core developers. Furthermore, the rigid "Code is Law" model proved fatally *brittle*. The canonical example of "The DAO" hack of 2016 demonstrated that in moments of crisis, the community must abandon algorithmic absolutism and rely on *off-chain social consensus*, a human political process, to intervene (e.g., via a hard fork). This revealed that human judgment remains a *sovereign* in these systems.

The final chapter served as the *legal reckoning* for this failed experiment, analyzing the collision between DAOs and corporate law. The core finding is that a "native" DAO represents a "Legal Misfit" of catastrophic proportions, failing to map onto the five foundational attributes of the modern corporation. It lacks Legal Personality, rendering it unable to own property, sign contracts, or appear in court. Most critically, it lacks Limited Liability. Without a legal wrapper, it defaults to a general partnership, exposing *all* voting token holders to unlimited personal liability, as confirmed in cases like *CFTC v. Ooki DAO*. It also lacks functional Delegated Management, as its attempts to reinvent delegation occur *without* legally imposed fiduciary duties, leaving participants unprotected. Its concept of Investor Ownership is ambiguous, with token holders lacking clear, enforceable claims on profits or assets. Lastly, for the transferable shares attribute of the modern corporation, while tokens offer hyper-transferability, this creates regulatory chaos (securities law) and governance instability. In synthesis, the revolutionary *ideology* (Chapter 1) was *tamed* by the state (Chapter 2), *failed* its own governance tests (Chapter 3), and was *legally neutralized* by corporate law, which re-imposed punitive liability (Chapter 4). The "rule of law" remains supreme over "code is law."

6.2 Recommendations

The theoretical insights and empirical findings synthesized throughout this thesis converge on a set of actionable and prescriptive recommendations for legislators, regulators, public agencies, and DAO communities seeking to navigate the complex intersection of blockchain technology, law, and governance. These recommendations form a practical playbook aimed at fostering responsible innovation while upholding fundamental legal principles and ensuring accountability.

For Public Sector Implementation, the primary recommendation is to adopt a problem-driven, not technology-driven, approach. The decision to deploy blockchain technology must originate from a strategic assessment of a genuine institutional coordination problem where trust or intermediation costs are the core issue, not from a fascination with the technology itself. Administrations must conduct rigorous suitability, scalability, and feasibility evaluations comparing blockchain against simpler, centralized alternatives, particularly questioning its appropriateness for functions requiring policy flexibility or interpretive discretion, where immutability becomes a liability.

Secondly, establishing legal clarity and certainty is paramount. Legislators must proactively update frameworks to formally recognize the validity of blockchain-notarized data and digital signatures for public functions. Critically, the legal roles and responsibilities within blockchain ecosystems, especially identifying the "controller" under data protection law, must be clearly defined to ensure accountability. Failure to provide this foundational legal certainty remains the single greatest bottleneck preventing successful pilots from scaling.

Third, public policy should mandate standards-based interoperability and promote open architectures. To avoid creating new digital silos and prevent vendor lock-in, procurement guidance must prioritize open-source software and support international standards for security, privacy, and governance. Initiatives like the European Blockchain Service Infrastructure (EBSI) offer a model for developing foundational components that enable scalable, cross-border public services.

Fourth, audit regimes must be strengthened, and legal safeguards embedded by design. The automation inherent in blockchain requires robust, independent, human-centric oversight. Legal principles, especially data protection, cannot be afterthoughts; they demand proactive integration through rigorous Impact Assessments (e.g., DPIAs) conducted *before* deployment. Crucially, strong off-chain governance mechanisms must be established for dispute resolution, providing explanations for automated decisions, and preserving the right to effective judicial review.

Finally, governments must invest significantly in institutional capacity and foster strategic partnerships. The greatest barriers are organizational inertia and skill gaps. Public administrations need to build in-house knowledge to act as intelligent clients, even when development is outsourced. This requires partnerships with academia and the private sector, coupled with comprehensive training for public officials to ensure they can effectively govern and oversee these complex systems.

For Decentralized Autonomous Organizations (DAOs) and the regulators grappling with them, the recommendations focus on bridging the "Legal Misfit." The most urgent priority is addressing the liability crisis. Legislatures should move beyond the disastrous default of general partnership law and develop bespoke legal forms that offer DAOs a pathway to achieve legal personality and limited liability. These forms must be carefully designed to accommodate decentralized governance structures while still ensuring accountability.

Exploring hybrid structures that integrate on-chain governance with recognized off-chain legal entities (like the DAO LLC or Swiss Foundation models) offers a pragmatic transitional solution. Future refinements should focus on clarifying the legal relationship between token-holder votes and the fiduciary duties of any designated managers or administrators, preserving decentralization while ensuring enforceability.

International cooperation is essential to develop harmonized principles for global recognition, potentially building on frameworks like the COALA Model Law for DAOs. Such principles should include minimum standards for transparency (e.g., public code repositories, audited smart contracts) and governance documentation, potentially linking automatic conferral of limited liability to compliance with these standards. This approach could mitigate the jurisdictional patchwork that currently plagues the ecosystem.

Regulators should transition towards functional and risk-based regulation. Instead of focusing narrowly on the technological architecture (blockchain vs. database), assessment should center on the *nature and impact* of the DAO's economic activity. Regulatory obligations should be calibrated proportionally to the systemic risk posed, mirroring approaches used in financial regulation. Initiatives like regulatory sandboxes are valuable for testing these approaches, allowing innovation under supervised conditions.

Finally, DAO communities themselves must proactively embrace robust internal governance standards. This includes adopting clear, natural-language charters alongside their code, establishing transparent off-chain dispute resolution mechanisms, and potentially experimenting with governance models beyond simple token-weighted voting (e.g., quadratic voting, reputation-based systems) to mitigate plutocratic capture and enhance input legitimacy. Self-regulation and adherence to best practices will be crucial for building trust and demonstrating viability to regulators and the broader public.

6.3 Contributions, Limitations, and Future Research

This thesis contributes novel theoretical frameworks (the "Governance Paradox" and "Legal Misfit"), provides a holistic interdisciplinary synthesis across philosophy, public law, economics, organizational theory, and corporate law, and offers a sober, evidence-based corrective to technoutopian narratives by highlighting critical risks and documented failures. However, its conclusions are subject to limitations stemming from the rapidly evolving nature of the field (the "moving target" problem), its reliance on a literature-based synthesis rather than primary qualitative data, and its focused, though not exhaustive, jurisdictional scope.

These limitations point directly toward urgent avenues for future research. Longitudinal studies are needed to track the long-term impact and sustainability of public sector blockchain projects. Qualitative ethnographies are essential to uncover the off-chain human dynamics and power negotiations that truly drive DAO governance. Deep comparative legal analysis of emerging bespoke DAO laws across jurisdictions is critical to assess their effectiveness and cross-border compatibility. Finally, anticipating the next technological wave, research must explore the profound legal and governance challenges posed by the intersection of AI and DAOs, particularly regarding autonomous AI agents acting within these decentralized structures.

In the final analysis, the story of blockchain's encounter with established governance frameworks is one of a radical technology being gradually domesticated by the enduring power of law and institutional norms. While it offers powerful tools for coordination and transparency, it is not a substitute for the rule of law, democratic accountability, or the necessity of human judgment. The future viability of both government blockchains and DAOs will hinge not on cryptographic elegance alone, but on their clear and unwavering integration within robust legal frameworks that uphold constitutional principles and ensure human accountability. The ongoing challenge is to design and govern these potent systems in a manner that strengthens, rather than subverts, the societal commitments they are ultimately meant to serve.

Bibliography

- Akgiray, V. (2019). *The potential for blockchain technology in corporate governance*.
- Alessie, D., Sobolewski, M., & Vaccari, L. (2019). *Blockchain for digital government*. Publications Office of the European Union.
- Alexander C. Drylewski. (2023, April 3). *Court Ruling Could Affect the Future Direction of DAOs*. Skadden. <https://www.skadden.com/insights/publications/2023/04/court-ruling-could-affect-the-future-direction-of-daos>
- Allen, D. W., & Berg, C. (2020). Blockchain governance: What we can learn from the economics of corporate governance. *The Journal of The British Blockchain Association*.
- Allen, D. W., Berg, C., & Lane, A. M. (2019). *Cryptodemocracy: How blockchain can radically expand democratic choice*. Bloomsbury Publishing PLC.
- Allen, J. G. (2020). Bodies without organs: Law, economics, and decentralised governance. *Stan. J. Blockchain L. & Pol'y*, 4, 53.
- Alston, E. (2019). Constitutions and blockchains: Competitive governance of fundamental rule sets. *Case W. Res. JL Tech. & Internet*, 11, 131.
- Alston, E. (2022). Blockchain and the law-legality, law-like characteristics, and legal applications. *The Economics of Blockchain and Cryptocurrency*, 117–144.
- Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2022). Blockchain networks as constitutional and competitive polycentric orders. *Journal of Institutional Economics*, 18(5), 707–723.
- Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media, Inc.
- Aragon. (n.d.). *Aragon*. Retrieved November 10, 2025, from <https://app.aragon.org/?daoFilter=all>
- Armour, J., Hansmann, H., & Kraakman, R. (2009). *Essential Elements of Corporate Law*.

- Armour, J., Hansmann, H., Kraakman, R., & Pargendler, M. (2017). Foundations of corporate law. *FGV Direito SP Research Paper Series*, 147.
- Assange, J., Appelbaum, J., Muller-Maguhn, A., & Zimmermann, J. (2016). *Cypherpunks: Freedom and the Future of the Internet*. OR books.
- Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, 6(1), 45-62,.
- Axelsen, H., Jensen, J. R., & Ross, O. (2023). When is a DAO Decentralized? *arXiv Preprint arXiv:2304.08160*.
- Back, A. (2002). *Hashcash-a denial of service counter-measure*.
- Bank of Canada, & Monetary Authority of Singapore. (2019). *Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies*. <https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf>
- Bank of International Settlements Basel Committee. (2021). *Prudential treatment of cryptoasset exposures*. <https://www.bis.org/bcbs/publ/d545.htm>
- Bannister, A. (2021, November 9). *bZx crypto heist results in reported losses of more than \$55 million*. The Daily Swig. <https://portswigger.net/daily-swig/bzx-crypto-heist-results-in-reported-losses-of-more-than-55-million>
- Barak, A., & Kalir, D. (2012). Proportionality: Constitutional rights and their limitations. (*No Title*).
- Barbureau, T., Smethurst, R., Papageorgiou, O., Rieger, A., & Fridgen, G. (2022). *Defi, not so decentralized: The measured distribution of voting rights*.

- Barbureau, 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.
- Barbrook, R., & Cameron, A. (1996). The californian ideology. *Science as Culture*, 6(1), 44–72.
- Barbrook, R., & Cameron, A. (2015). *The Internet Revolution: From dot-com capitalism to cybernetic communism*. Institute of Network Cultures.
- Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*.
<https://www.eff.org/cyberspace-independence>
- Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1-9,.
- Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 19(10), 1020–1034.
- Becker, K. (2022). Blockchain matters—Lex cryptographia and the displacement of legal symbolics and imaginaries. *Law and Critique*, 33(2), 113–130.
- Becker, M., & Bodó, B. (2021a). Trust in blockchain-based systems. *Internet Policy Review*, 10(2).
<https://doi.org/10.14763/2021.2.1555>
- Becker, M., & Bodó, B. (2021b). Trust in blockchain-based systems. *Internet Policy Review*, 10(2).
- Beckett, J. (2023). Wyoming DAO LLC Overview Timeline of Digital Asset Law in Wyoming. In *DECENTRALISED AUTONOMOUS ORGANISATIONS (DAOS) IN VARIOUS JURISDICTIONS: FROM OLD RULES TO INNOVATIVE APPROACHES*.

- Bell, T. W. (2021). Blockchain and authoritarianism: The evolution of decentralized autonomous organizations. In *Blockchain and Public Law* (pp. 90–104). Edward Elgar Publishing.
- Bellavitis, C., Fisch, C., & Momtaz, P. P. (2023). The rise of decentralized autonomous organizations (DAOs): A first empirical glimpse. *Venture Capital*, 25(2), 187–203.
- Belleflamme, P., & Peitz, M. (2018). *Platforms and network effects*. Edward Elgar Publishing.
- Berryhill, J., Bourgerie, T., & Hanson, A. (2018). *Blockchains unchained: Blockchain technology and its use in the public sector*.
- Biondi Santi, C., & Vespri, V. (2020). Solving Cryptographic Puzzles: How to Mine? In *Blockchain, Law and Governance* (pp. 73–84). Springer.
- Bitcoin Magazine. (2018, March 6). *Switzerland's "Crypto Valley" Successfully Completes Blockchain Voting Trial*. <https://www.nasdaq.com/articles/switzerlands-crypto-valley-successfully-completes-blockchain-voting-trial-2018-07-03>
- Biyan Mienert. (2024). Limited Liability as Applied to DAOs. In *Decentralised Autonomous Organisation (DAO) Regulation Principles and Perspectives for the Future*. <https://library.oapen.org/handle/20.500.12657/93753>
- Blemus, S. (2023). DAO and Private International Law: Preliminary reflections from a French law perspective. In *Decentralised Autonomous Organisations (DAOs) in Various Jurisdictions: From Old Rules to Innovative Approaches*. <https://www.cidp.pt/publication/decentralised-autonomous-organisations-daos-in-various-jurisdictions-from-old-rules-to-innovative-approaches/292>
- Bodó, B. (2021). The commodification of trust. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3843707>

- Bodó, B., & Janssen, H. (2022). Maintaining trust in a technologized public sector. *Policy and Society*, 41(3), 414–429. <https://doi.org/10.1093/polsoc/puac019>
- Boeding, K. (2024). 3 Potential Benefits of Blockchain for Government. Booz Allen. <https://www.boozallen.com/s/insight/blog/3-potential-benefits-of-government-blockchain.html>
- Bohme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238.
- Borgogno, O., & Martino, E. D. (2024). *Decentralised Autonomous Organizations: Targeting the Potential Beyond the Hype*.
- Bosch, J. M., Tangi, L., & Burian, P. (2022). *European landscape on the use of blockchain technology by the public sector*. Joint Research Centre.
- Boss, S. (2023). DAOs: Legal and Empirical Review. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4503234>
- Brekke, J. K. (2021). Hacker-engineers and their economies: The political economy of decentralised networks and ‘cryptoeconomics.’ *New Political Economy*, 26(4), 646–659.
- Brennecke, M., Guggenberger, T., Schellinger, B., & Urbach, N. (2022). *The de-central bank in decentralized finance: A case study of MakerDAO*.
- Brinkmann, M. (2021). The realities of blockchain-based new public governance: An explorative analysis of blockchain implementations in Europe. *Digital Government: Research and Practice*, 2(3), 1–14.
- Brook Knight, T. (2017, June 14). *Financial Alphabet Soup*. CATO Institute. <https://www.cato.org/blog/financial-alphabet-soup>
- Brummer, C., & Seira, R. (2022). Legal wrappers and DAOs. *Available at SSRN*.

- Business & Information Systems Engineering of the Fraunhofer FIT, & Interdisciplinary Centre for Security, Reliability, and Trust of the University of Luxembourg. (2022). *Opportunities and challenges of using blockchain technology in public administration*. https://www.bamf.de/SharedDocs/Anlagen/EN/Digitalisierung/blockchain-whitepaper-Chancen-Herausforderungen.pdf?__blob=publicationFile&v=5
- Bustamante, P., Cai, M., Gomez, M., Harris, C., Krishnamurthy, P., Law, W., Madison, M. J., Murtazashvili, I., Murtazashvili, J. B., & Mylovanov, T. (2022). Government by code? Blockchain applications to public sector governance. *Frontiers in Blockchain*, 5, 869665.
- Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*.
- Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for public services: A systematic literature review. *IEEE Access*, 9, 13904-13921,.
- Campbell-Verduyn, M. (2017). Introduction: What are blockchains and how are they relevant to governance in the global political economy? In *Bitcoin and beyond* (pp. 1–24). Routledge.
- Campbell-Verduyn, M. (2018). *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. Routledge.
- Cappiello, B., & Carullo, G. (2021). *Blockchain, law and governance*. Springer.
- Caradonna, T. (2020). Blockchain and society. *Informatik Spektrum*, 43(1), 40–52.
- Castells, M., & Cardoso, G. (1996). *The network society* (Vol. 469). Oxford: blackwell.
- Cervone, L., Palmirani, M., & Vitali, F. (2020). *The Intelligible Contract*. 1–10.
- Chainalysis. (2022, February 3). *Smart Contract Vulnerabilities Introduce Risk; Blockchains' Transparency Makes It Hard for Bad Actors to Cash Out*. <https://www.chainalysis.com/blog/wormhole-hack-february-2022/>

- Chainlink. (2025). *What Is a Blockchain Oracle?* <https://chain.link/education/blockchain-oracles>
- Charlton, G. C., Adams, M., & Whang, C. (2023). The Decentralised Autonomous Organization: Legal Personality and the Problem of Governance. *JL & Com.*, 42, 55.
- Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology*, 199–203.
- Chaum, D., & Brands, S. (1997). 'Minting' electronic cash. *IEEE Spectrum*, 34(2), 30–34.
- Chavez-Dreyfuss, G. (2021, August 12). *How hackers stole \$613 million in crypto tokens from Poly Network.* <https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/>
- Citron, D. K. (2007). Technological due process. *Wash. UL Rev.*, 85, 1249.
- Clayton, R., Murdoch, S. J., & Watson, R. N. (2006). *Ignoring the great firewall of china.* 20–35.
- Clifton, J., & Pal, L. A. (2022). The policy dilemmas of blockchain. *Policy and Society*, 41(3), 321–327.
- Coase, R. H. (2012). The nature of the firm. In *The roots of logistics* (pp. 317–333). Springer.
- Commodity Futures Trading Commission. (2022a). *CFTC Order Finds, and Complaint Alleges, Ooki DAO is Liable as an Unincorporated Association* (Press Release Nos. 8590–22). <https://www.cftc.gov/PressRoom/PressReleases/8590-22>
- Commodity Futures Trading Commission. (2022b). *CFTC Order Finds, and Complaint Alleges, Ooki DAO is Liable as an Unincorporated Association.* <https://www.cftc.gov/PressRoom/PressReleases/8590-22>
- Commodity Futures Trading Commission. (2023). *Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory* (Press Release Nos. 8715–23). <https://www.cftc.gov/PressRoom/PressReleases/8715-23>

- Connelly, B. L., Hoskisson, R. E., Tihanyi, L., & Certo, S. T. (2010). Ownership as a form of corporate governance. *Journal of Management Studies*, 47(8), 1561–1589.
- Cryptopedia Staff. (2023, October 5). *SushiSwap and Vampire Attacks in Decentralized Finance (DeFi)*. Cryptopedia. <https://www.gemini.com/cryptopedia/sushiswap-uniswap-vampire-attack>
- Dai, W. (1998). *B-money*.
- DAOHAUS. (n.d.). *DAOHAUS*. Retrieved November 10, 2025, from <https://daohaus.club>
- Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4), 639–658.
- Davis, K. C. (1969). *Discretionary justice: A preliminary inquiry*. LSU Press.
- Day, M. S. (2018). *Bits to bitcoin: How our digital stuff works*. MIT Press.
- de Caria, R. (2021). Blockchain and sovereignty. In *Blockchain and Public Law* (pp. 41–59). Edward Elgar Publishing.
- De Filippi, P., Mannan, M., Nabben, K., Cossar, S., Kamalova, J., Merk, T., Noa, S., Crepaldi, M., & Dávila, J. (2023). Blockchain Constitutionalism: The Role of Legitimacy in Polycentric Systems. *EUI: Florence, Italy*.
- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, 62, 101284. <https://doi.org/10.1016/j.techsoc.2020.101284>
- De Filippi, P., Mannan, M., & Reijers, W. (2022). The a legality of blockchain technology. *Policy and Society*, 41(3), 358–372.
- De Filippi, P., Mannan, M., & Reijers, W. (2024). *Blockchain governance*. MIT Press.

- De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.
- De Gregorio, G. (2021). Blockchain and freedom of expression. In *Blockchain and Public Law* (pp. 123–140). Edward Elgar Publishing.
- De Hert, P., & Kumar, A. (2021). Blockchain, privacy, and data protection. In *Blockchain and Public Law* (pp. 141–156). Edward Elgar Publishing.
- de Oliveira, M. P., & Rolo, A. G. (2023). *Decentralised Autonomous Organisations (DAOs) in Various Jurisdictions: From Old Rules to Innovative Approaches*.
<https://www.cidp.pt/publication/decentralised-autonomous-organisations-daos-in-various-jurisdictions-from-old-rules-to-innovative-approaches/292>
- de Sousa, J. S. (2024). Decentralized autonomous organisations (DAOs) and knowledge attribution. In *Decentralised Autonomous Organisation (DAO) Regulation Principles and Perspectives for the Future*.
https://www.csassociados.pt/xms/files/v2/Conhecimento_2024/Decentralised_Autonomous_Organisation_-DAO-_Regulation.pdf
- DeepDao. (n.d.). *DAO Statistics*.
- Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, 11(1), 51–64.
- Dicey, A. V., & Wade, E. C. S. (1939). *Introduction to the Study of the Law of the Constitution*. HeinOnline.
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/lqr55&div=42&id=&page=>

- DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social implications of the Internet. *Annual Review of Sociology*, 27(1), 307–336.
- Dimitropoulos, G. (2020). The law of blockchain. *Wash. L. Rev.*, 95, 1117.
- Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. *Healthcare Informatics Research*, 25(1), 51–56.
- DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of “the dao,” a failed decentralized autonomous organization. *Bitcoin and beyond*, Routledge, 157–177.
- Dyson, E. (1996). Cyberspace and the American dream: A magna carta for the knowledge Age (release 1.2, August 22, 1994). *The Information Society*, 12(3), 295–308.
- Easterbrook, F. H., & Fischel, D. R. (1985). Limited liability and the corporation. *U. Chi. L. Rev.*, 52, 89.
- Easterbrook, F. H., & Fischel, D. R. (1996). *The economic structure of corporate law*. Harvard university press.
- e-Estonia. (n.d.). *E-Health*. Retrieved March 10, 2025, from <https://e-estonia.com/solutions/e-health-2/e-health-records/>
- El Faqir, Y., Arroyo, J., & Hassan, S. (2020). *An overview of decentralized autonomous organizations on the blockchain*. 1–8.
- Electronic Frontier Foundation. (n.d.). *Bernstein v. US Department of Justice*. <https://www EFF.org/cases/bernstein-v-us-dept-justice>
- Electronic Frontier Foundation. (2025). *The Crypto Wars*. https://www EFF.org/files/2025/08/19/the_crypto_wars.pdf

- European Commission. (n.d.). *What is the rule of law?* European Commission. Retrieved September 17, 2025, from https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/what-rule-law_en
- Eyal, I., & Sirer, E. (2014). *Financial Cryptography and Data Security*. 3–7.
- Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law and Economics*, 26(2), 301–325.
- Faqir-Rhazoui, Y., Arroyo, J., & Hassan, S. (2021). A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. *Journal of Internet Services and Applications*, 12(1), 9. <https://doi.org/10.1186/s13174-021-00139-6>
- Featherstone, M., & Burrows, R. (1995). *Cyberspace/Cyberbodies/Cyberpunk: Cultures of Technological Embodiment*. Sage Publications.
- Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Cambridge University Press.
- Fischer, A., & Valiente, M.-C. (2021). Blockchain governance. *Internet Policy Review*, 10(2), 1–10.
- Florian Möslin & Daniel Ostrovski. (2024). Legal personality of Decentralized Autonomous Organisations (DAOs): Privilege or Necessity? In *Decentralised Autonomous Organisation (DAO) Regulation: Principles and Perspectives for the Future*. <https://library.oapen.org/handle/20.500.12657/93753>
- Fracassi, C., Khoja, M., & Schär, F. (2024). Decentralized crypto governance? Transparency and concentration in Ethereum decision-making. *Transparency and Concentration in Ethereum Decision-Making (January 10, 2024)*.

- Fridgen, G., Guggenmos, F., Lockl, J., RIEGER, A., & Urbach, N. (2019). *Supporting communication and cooperation in the asylum procedure with Blockchain technology: A proof of concept by the Federal Office for Migration and Refugees*. <https://eref.uni-bayreuth.de/48037/>
- Fritsch, R., Müller, M., & Wattenhofer, R. (2024). Analyzing voting power in decentralized governance: Who controls DAOs? *Blockchain: Research and Applications*, 5(3), 100208.
- Ganado, M. (2023). Malta's Tentative Steps Towards DAO Personification. In *Decentralised Autonomous Organisations (DAOs) in Various Jurisdictions: From Old Rules to Innovative Approaches*. <https://www.cidp.pt/publication/decentralised-autonomous-organisations-daos-in-various-jurisdictions-from-old-rules-to-innovative-approaches/292>
- Geiser, U. (2021, July 3). *Digital identity scheme shot down by voters over data privacy concerns*. Swissinfo.Ch. <https://www.swissinfo.ch/eng/politics/digital-identity-scheme-faces-scepticism-around-data-privacy/46399636>
- Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 3–16.
- Gilbert, H., & Handschuh, H. (2003). *Security analysis of SHA-256 and sisters*. 175–193.
- Goossens, J. (2021). Blockchain and democracy: Challenges and opportunities of blockchain and smart contracts for democracy in the distributed, algorithmic state. In *Blockchain and Public Law*. Edward Elgar Publishing.
- G'sell, F., & Martin-Bariteau, F. (2022). The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law. *Report, Council of Europe*.
- Guegan, D. (2017). *Public blockchain versus private blockchain*.

- Hacker, P. (2019). *Corporate governance for complex cryptocurrencies? A framework for stability and decision making in blockchain-based organizations.*
- Han, J., Lee, J., & Li, T. (2025). A review of DAO governance: Recent literature and emerging trends. *Journal of Corporate Finance*, 102734.
- Hansmann, H. (2000). *The ownership of enterprise*. Harvard University Press.
- Harris, R. (2020). A new understanding of the history of limited liability: An invitation for theoretical reframing. *Journal of Institutional Economics*, 16(5), 643–664.
- Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, 10(2), 1–10.
- Hermstrüwer, Y. (2021). Blockchain and public administration. In *Blockchain and Public Law*. <https://www.elgaronline.com/edcollbook/edcoll/9781839100789/9781839100789.xml>
- Hester M. Peirce. (2021, April 13). *Token Safe Harbor Proposal 2.0*. U.S. Securities and Exchange Commission. <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-token-safe-harbor-proposal-20>
- Hillis, K., Petit, M., & Jarrett, K. (2012). *Google and the Culture of Search*. Routledge.
- Hobbes, T., & Missner, M. (2016). *Thomas Hobbes: Leviathan (Longman library of primary sources in philosophy)*. Routledge.
- Hoffman, R. (2015, May 15). *Reid Hoffman: Why the blockchain matters*. Wired. <https://www.wired.com/story/bitcoin-reid-hoffman/>
- Hood, C. (1995). The “new public management” in the 1980s: Variations on a theme. *Accounting, Organizations and Society*, 20(2–3), 93–109.
- Hsieh, Y., & Vergne, J. (2023). The future of the web? The coordination and early-stage growth of decentralized platforms. *Strategic Management Journal*, 44(3), 829–857.

- Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, 7(1), 1–16.
- Hsieh, Y.-Y., Vergne, J.-P. J., & Wang, S. (2017). The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. In *Bitcoin and beyond* (pp. 48–68). Routledge.
- Hughes, E. (1993). *A Cypherpunk's Manifesto*.
<https://www.activism.net/cypherpunk/manifesto.html>
- Jensen, M. C., & Meckling, W. H. (2019). Theory of the firm: Managerial behavior, agency costs and ownership structure. In *Corporate governance* (pp. 77–132). Gower.
- Juodis, M., Filatovas, E., & Paulavičius, R. (2024). Overview and empirical analysis of wealth decentralization in blockchain networks. *ICT Express*, 10(2), 380–386.
- Kaal, W. A. (2019). Blockchain Solutions for Agency Problems in Corporate Governance. *RCRN: Agency (Topic)*.
- Kelsen, H. (2017). *General theory of law and state*. Routledge.
- Khan, D., Jung, L., & Hashmani, M. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*. <https://doi.org/10.3390/app11209372>
- Kitzler, S., Baliotti, S., Saggese, P., Haslhofer, B., & Strohmaier, M. (2024). *The governance of decentralized autonomous organizations: A study of contributors' influence, networks, and shifts in voting power*. 313–330.
- Kohl, U. (2021). Blockchain utopia and its governance shortfalls. In *Blockchain and Public Law* (pp. 13–40). Edward Elgar Publishing.

- Komorowski, M., Claeys, L., & Van Dam, T. (2022). *DIGITAL DECENTRALIZED TRANSFER OF VALUE FOR THE PUBLIC SECTOR: a playing field analysis: How can Distributed Ledger Technologies like blockchain impact public values?*
- Kraakman, R. H., Armour, J., Davies, P., & Enriques, L. (2017). *The anatomy of corporate law: A comparative and functional approach*. Oxford university press.
- Kraken. (2024). *What are Layer 2 solutions?* <https://www.kraken.com/learn/layer-2-solutions>
- Lee Pascoe. (2023, April 28). *Decentralised autonomous organisations and liability in litigation – Sarcuni, et al v bZx DAO, et al*. International Bar Association. <https://www.ibanet.org/decentralised-autonomous-organisations-and-liability-in-litigation>
- Lehar, A., & Parlour, C. A. (2022). *Systemic fragility in decentralized markets*. Bank for International Settlements, Monetary and Economic Department.
- Lessig, L. (2009). *Code: And other laws of cyberspace*. ReadHowYouWant. com.
- Lianos, I. (2019). *Blockchain Competition—Gaining Competitive Advantage in the Digital Economy: Competition Law Implications*. Oxford University Press.
- Linde, H. A. (1975). Due process of lawmaking. *Neb. L. Rev.*, 55, 197.
- Liu, L., Zhou, S., Huang, H., & Zheng, Z. (2021). From technology to society: An overview of blockchain-based DAO. *IEEE Open Journal of the Computer Society*, 2, 204–215.
- Liu, Y., He, J., Li, X., Chen, J., Liu, X., Peng, S., Cao, H., & Wang, Y. (2024). An overview of blockchain smart contract execution mechanism. *Journal of Industrial Information Integration*, 41, 100674.
- Liu, Y., Lu, Q., Yu, G., Paik, H.-Y., & Zhu, L. (2022). Defining blockchain governance principles: A comprehensive framework. *Information Systems*, 109, 102090.

- Liu, Y., Lu, Q., Zhu, L., Paik, H.-Y., & Staples, M. (2023). A systematic literature review on blockchain governance. *Journal of Systems and Software*, 197, 111576.
- Ljungberg, J. (2000). Open source movements as a model for organising. *European Journal of Information Systems*, 9(4), 208–216.
- Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance—A new way of organizing collaborations? *Organization Science*, 32(2), 500–521.
- Magnuson, W. (2020). *Blockchain Democracy*. Cambridge University Press.
- MakerDAO. (n.d.). The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. *MakerDAO*. <https://makerdao.com/en/whitepaper/#abstract>
- Malone, T. W., Yates, J., & Benjamin, R. I. (1987). Electronic markets and electronic hierarchies. *Communications of the ACM*, 30(6), 484–497.
- Manne, H. G. (1967). Our two corporation systems: Law and economics. *Virginia Law Review*, 259–284.
- Manne, R. (2020). The Cypherpunk Revolutionary. *The Monthly*, March 2011.
- Marsch, N., & Tümsmeyer, V. (2015). The principle of proportionality in German administrative law. In *The Judge and the Proportionate Use of Discretion* (pp. 13–42). Routledge.
- Maurer, B., Nelms, T. C., & Swartz, L. (2013). “When perhaps the real problem is money itself!”: The practical materiality of Bitcoin. *Social Semiotics*, 23(2), 261–277. <https://doi.org/10.1080/10350330.2013.777594>
- May, T. C. (1992). *The Crypto Anarchist Manifesto*. <https://www.activism.net/cypherpunk/crypto-anarchy.html>
- Mayer-Schönberger, V. (2011). Delete: The virtue of forgetting in the digital age. In *Delete*. Princeton University Press.

- Means, G. (2017). *The modern corporation and private property*. Routledge.
- Millon, D. (1990). Theories of the Corporation. *Duke LJ*, 201.
- Mondoh, B. S., Johnson, S. M., Green, M., & Georgopoulos, A. (2022). Decentralised autonomous organisations: The future of corporate governance or an illusion? *Aris (Aristeidis), Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion*.
- Morrison, R., Mazey, N. C. H. L., & Wingreen, S. C. (2020). The DAO Controversy: The Case for a New Species of Corporate Governance? *Frontiers in Blockchain*, 3(25).
- Mssassi, S., & Abou El Kalam, A. (2024). The blockchain trilemma: A formal proof of the inherent trade-offs among decentralization, security, and scalability. *Applied Sciences*, 15(1), 19.
- Nabben, K. (2021). Is a “Decentralized Autonomous Organization” a Panopticon? *Blockchain Innovation Hub*.
- Nai, A. (n.d.). *Access to Justice and Electoral Integrity*. Retrieved August 9, 2025, from <https://www.kofiannanfoundation.org/wp-content/uploads/2016/11/EII-Policy-Brief-3-Access-to-Justice-and-Electoral-Integrity.pdf>
- Nakai, T., Sakurai, A., Hironaka, S., & Shudo, K. (2024). A formulation of the trilemma in proof of work blockchain. *IEEE Access*, 12, 80559–80578.
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
- Naudts, E. (2023). The Future of DAOs in Finance—In Need of Legal Status. *European Central Bank Occasional Paper Series*, 331. <https://doi.org/10.2139/ssrn.4605627>

- Nunes Teixeira, A. (2023). DAOs Under Portuguese Law. In *Decentralised Autonomous Organisations (DAOs) in Various Jurisdictions: From Old Rules to Innovative Approaches*.
- Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, 34(3), 355–364.
- Osborne, S. P. (2006). *The new public governance? 1*.
- Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge university press.
- Paquet, G., & Wilson, C. (2015). GOVERNANCE FAILURE AND ANTIGOVERNMENT PHENOMENA. *Optimum Online*, 45(2).
- Parkin, J. (2020). *Money code space: Hidden power in Bitcoin, blockchain, and decentralisation*. Oxford University Press.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Peder Østbye. (2024). DAOs and Civil Liability. Some Policy Considerations. In *Decentralised Autonomous Organisation (DAO) Regulation Principles and Perspectives for the Future*. <https://library.oapen.org/handle/20.500.12657/93753>
- Pelt, R. van, Jansen, S., Baars, D., & Overbeek, S. (2021). Defining blockchain governance: A framework for analysis and comparison. *Information Systems Management*, 38(1), 21–41.
- Perestrelo de Oliveira, M., & Rolo, A. G. (2024). *Decentralised Autonomous Organisation (DAO) Regulation: Principles and Perspectives for the Future*.
- Pollicino, O., & De Gregorio, G. (2021). *Blockchain and public law: Global challenges in the era of decentralisation*. Edward Elgar Publishing.

- Poncibò, C. (2020). Blockchain and comparative law. In *Blockchain, law and governance* (pp. 137–156). Springer.
- Powell, W. W. (1990). *Neither Market Nor Hierarchy: Network Forms of Organization*. http://web.stanford.edu/~woodyp/powell_neither.pdf
- Puig, G. V. (2000). A two-edged sword: Salomon and the Separate Legal Entity Doctrine. *Murdoch University Electronic Journal of Law*, 7(3), 1–9.
- Racsko, P. (2019). Blockchain and democracy. *Society and Economy*, 41(3), 353–369.
- Raz, J. (2009). *The authority of law: Essays on law and morality*. Oxford University Press.
- Reddick, C. G., Rodríguez-Bolívar, M. P., & Scholl, H. J. (2021). *Blockchain and the Public Sector*. Springer.
- Reijers, W., & Coeckelbergh, M. (2018). The blockchain as a narrative technology: Investigating the social ontology and normative configurations of cryptocurrencies. *Philosophy & Technology*, 31(1), 103–130.
- Reijers, W., Wuisman, I., Mannan, M., Filippi, P. D., Wray, C., Rae-Looi, V., & Orgad, L. (2021). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi*, 40(4), 821–831,.
- Rhodes, R. A. W. (1996). The new governance: Governing without government. *Political Studies*, 44(4), 652–667.
- Rikken, O., Janssen, M., & Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. *Information Polity*, 24(4), 397–417.
- Riordan, M. H., & Williamson, O. E. (1985). Asset specificity and economic organization. *International Journal of Industrial Organization*, 3(4), 365–378.

- Riva, S. (2021). *Decentralized Autonomous Organizations (DAOs) in the Swiss Legal Order*. 601–638.
- Rossiter, C. (2017). *Constitutional dictatorship: Crisis government in the modern democracies*. Routledge.
- Rousseau, J.-J. (1913). *The social contract and discourses* (Issue 660). Dent.
- Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2021). When ostrom meets blockchain: Exploring the potentials of blockchain for commons governance. *Sage Open*, 11(1), 21582440211002526.
- Schillig, M. A. (2022). Decentralized Autonomous Organizations (DAOs) Under English law. *Law and Financial Markets Review*, 16(1–2), 68–78.
- Schmitt, C. (2005). *Political theology: Four chapters on the concept of sovereignty*. University of Chicago Press.
- Schwartz, A. A. (2011). The perpetual corporation. *Geo. Wash. L. Rev.*, 80, 764.
- Schwemmer, S. (2023). A legal form for DAOs under German Law. In *Decentralised Autonomous Organisations (DAOs) in Various Jurisdictions: From Old Rules to Innovative Approaches*.
- Schwiderowski, J., Pedersen, A. B., & Beck, R. (2024). Crypto tokens and token systems. *Information Systems Frontiers*, 26(1), 319–332.
- Securities and Exchange Commission. (2017). *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (No. 81207). <https://www.sec.gov/files/litigation/investreport/34-81207.pdf>
- Sharma, T., Potter, Y., Pongmala, K., Wang, H., Miller, A., Song, D., & Wang, Y. (2024). Future of Algorithmic Organization: Large-Scale Analysis of Decentralized Autonomous Organizations (DAOs). *arXiv Preprint arXiv:2410.13095*.

- Sims, A. (2019). *Blockchain and decentralised autonomous organisations (daos): The evolution of companies?*
- Sobolewski, M., & Allessie, D. (2021). Blockchain applications in the public sector: Investigating seven real-life blockchain deployments and their benefits. *Blockchain and the Public Sector: Theories, Reforms, and Case Studies*, 97–126.
- Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
- Swan, M., & De Filippi, P. (2017). Toward a philosophy of blockchain: A symposium: Introduction. *Metaphilosophy*, 48(5), 603–619.
- Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*.
- Tan, E., Mahula, S., & Cromptvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly*, 39(1).
- Tan, J. Z., Merk, T., Hubbard, S., Oak, E. R., Pirovich, J., Rennie, E., Hoefer, R., Zargham, M., Potts, J., & Berg, C. (2023). Open problems in daos. *arXiv Preprint arXiv:2310.19201*.
- Thompson, G. (1991). *Markets, hierarchies and networks: The coordination of social life*. Sage.
- Turner, F. (2024). *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. University of Chicago Press.
- Uniswap Foundation. (n.d.). *Uniswap governance*. Uniswap. Retrieved July 29, 2025, from <https://www.uniswapfoundation.org/governance>
- U.S. Department of Treasury. (2022). *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*. <https://home.treasury.gov/news/press-releases/jy0916>
- Vakarjuk, J., Snetkov, N., & Willemson, J. (2022). Russian Federal Remote E-voting Scheme of 2021 – Protocol Description and Analysis. *EICC 2022: Proceedings of the European*

- Interdisciplinary Cybersecurity Conference*, 29–35.
<https://doi.org/10.1145/3528580.3528586>
- Vandy, N. (2024). Progressive Decentralization requires Progressive Regulation: Do DAOs require direct legislative intervention, self-regulation or no regulation? In *Decentralised Autonomous Organisation (DAO) Regulation Principles and Perspectives for the Future*.
<https://library.oapen.org/handle/20.500.12657/93753>
- Varga, S., Cholakova, M., Jansen, J. J., Mom, T. J., & Kok, G. J. (2023). From platform growth to platform scaling: The role of decision rules and network effects over time. *Journal of Business Venturing*, 38(6), 106346.
- Vieira dos Santos, J. (2024). The Nature of the DAO: Transaction Costs, MiCA and a Specific Legal Framework. In *Decentralised Autonomous Organisation (DAO) Regulation Principles and Perspectives for the Future*.
<https://library.oapen.org/handle/20.500.12657/93753>
- Vitalik Buterin. (2017, December 31). Sharding FAQ. *Vitalik.Eth*.
https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html
- Wallace, B. (2011). The rise and fall of Bitcoin. *Wired*, 19(12).
- 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.
- Weber, M. (1922). *Economy and society* (Vol. 1).
- Weinstein, G., & Loftchie, S. (2022). *A Primer on DAOs*.
<https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/>
- Werbach, K. (2018). *Blockchain and the New Architecture of Trust*. MIT PRESS.

- Whiterabbit. (2020, March 14). *Black Thursday for MakerDAO: \$8.32 million was liquidated for 0 DAI*. Medium. https://medium.com/@whiterabbit_hq/black-thursday-for-makerdao-8-32-million-was-liquidated-for-0-dai-36b83cac56b6
- Williamson, O. E. (1981). The economics of organization: The transaction cost approach. *American Journal of Sociology*, 87(3), 548–577.
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. In *Ethereum Project Yellow Paper* (Vol. 151, pp. 1–32).
- World Economic Forum. (2020). *Exploring Blockchain Technology for Government Transparency*. https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf
- World Economic Forum. (2022). *Decentralized Autonomous Organizations: Beyond the Hype* (White Paper). World Economic Forum. <https://www.weforum.org/publications/decentralized-autonomous-organizations-beyond-the-hype/>
- World Economic Forum. (2023). *DAOs for Impact*. https://www3.weforum.org/docs/WEF_DAOs_for_Impact_2023.pdf
- Wright, A. (2021). *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*.
- Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31.
- Yeung, K. (2017). Blockchain, transactional security and the promise of automated law enforcement: The withering of freedom under law? *TLI Think*.
- Zein, D., & Pinkwart, Wi. (2025). *Leveraging Zero-Knowledge Proofs for GDPR Compliance in Blockchain Projects* (INATBA Position). International Association for Trusted Blockchain

- Applications. <https://inatba.org/wp-content/uploads/2025/08/Leveraging-ZKP-for-GDPR-Compliance-in-Blockchain-Projects.pdf>
- Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. *U. Ill. L. Rev.*, 1361.
- Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105, 475–491.
- Ziegler, C., & Welp, I. M. (2022). *A taxonomy of decentralized autonomous organizations*. ICIS 2022 proceedings.
- Zimmermann, P. (1995). *The Official PGP User's Guide*. MIT Press.
- Ziolkowski, R., Miscione, G., & Schwabe, G. (2020a). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems*, 37(2), 316–348.
- Ziolkowski, R., Miscione, G., & Schwabe, G. (2020b). Exploring decentralized autonomous organizations: Towards shared interests and 'code is constitution.' *Forty-First International Conference on Information Systems (ICIS)*.
- Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203–213). Routledge.
- Zwitter, A., & Hazenberg, J. (2020a). Cyberspace, blockchain, governance: How technology implies normative power and regulation. In *Blockchain, law and governance* (pp. 87–97). Springer.

- Zwitter, A., & Hazenberg, J. (2020b). Decentralized Network Governance: Blockchain Technology and the Future of Regulation. *Frontiers in Blockchain*, 3, 12. <https://doi.org/10.3389/fbloc.2020.00012>
- Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: Universal identity management and the concept of the “Self-Sovereign” individual. *Frontiers in Blockchain*, 3, 26.