Governance of Common Knowledge in Distributed Systems

Sara Malik, Grieg Greger, and Naveed A.A.

PakCrypt NPO
greig@pakcrypt.org

Abstract. We address a persistent, under-theorised problem at the intersection of distributed systems and governance: how to maintain trustworthy, tamper-evident shared state across parties who may not fully trust one another, not merely at deployment, but across the full lifecycle of a long-lived sociotechnical system. We call this the *Common-Knowledge Problem* (CKP) and define it precisely: CKP is the challenge of maintaining knowledge that would be knowable in principle—if authorised by policy and enabled by communication availability—where both the authorisation gate and the channel are governed by whichever entity or rule-based protocol a community has chosen to trust. We argue that the core difficulty is not cryptographic but *political*: the adversarial forces that degrade governance over time are precisely those analysed by 2,500 years of political philosophy. We propose a layered ontological model that decomposes any CKP system into five analytically separable strata, and maps eight canonical governance archetypes— drawn from Hobbes, Plato, Aristotle, Polybius, Rousseau, Weber, Michels, and Schmitt—onto that stack. For each archetype we identify its principle of legitimacy, its characteristic *decay vector*, and the conditions under which it constitutes a correct engineering choice. We further derive eight cross-cutting decay laws and a six-step diagnostic procedure for practitioners. Our synthesis is empirically grounded: we test each predicted decay path against documented modern cases in blockchain governance, certificate-authority politics, DAO voter concentration, and enterprise change management. The framework yields a practical method for selecting, instrumenting, and periodically re-diagnosing a governance structure suited to a given threat model and responsible-ownership context.

Keywords: Common-Knowledge Problem · Cyber Governance · Distributed Ledger · Blockchain Governance · Political Philosophy · Ontological Framework · Trust · Decentralisation

1 Introduction

Every system designed to maintain a shared, authoritative record—from a national land registry to a public blockchain—faces a governance problem that outlasts its technical design. Cryptographic primitives, consensus protocols, and

access-control policies can be specified and verified at deployment; what cannot be specified once and then left unattended is the *political life* of the system: the question of who controls the rules, how those controllers are selected and held accountable, and how the system evolves when its environment changes or when powerful actors seek to bend it to their advantage.

We term the underlying epistemic objective the *Common-Knowledge Problem* (CKP). Drawing on Aumann's [1] formal definition of common knowledge and the Halpern–Moses impossibility result [2], we establish that no real system can deliver strict common knowledge; every system instead delivers a *bounded approximation*—verifiable shared state with an explicit finality rule—and governance is the management of the two gaps: between the approximation and the ideal, and between the stated finality rule and the actors who can override it.

Our central thesis is that this governance problem is structurally isomorphic to the problems analysed by the canonical tradition of political philosophy. Both domains confront rational, self-interested actors, asymmetric information, long time horizons, and the possibility that the authority responsible for maintaining the record is itself the most dangerous adversary. Political philosophy is therefore not an analogy for, but a *primary empirical source* about, how governance structures succeed, fail, and decay.

The paper makes four principal contributions. First, we provide a layered ontological model (Sect. 4) that separates the technical and political strata of a CKP system and locates governance at the stratum where it actually operates. Second, we develop eight governance archetypes (Sect. 5), each grounded in canonical primary sources, calibrated against documented historical cases, and stress-tested against modern digital-governance incidents. Third, we synthesise eight cross-cutting decay laws (Sect. 6) that act on every archetype and that must be instrumented against rather than assumed away. Fourth, we provide a six-step applied diagnostic procedure (Sect. 8) that translates the ontology into a practical selection and monitoring method.

We take care throughout to identify where the political-philosophy analogy leaks—where the structural differences between territorial polities and digital protocols invalidate a direct transfer—so that practitioners do not import the metaphor's *ceremony* in place of its *content*.

2 The Common-Knowledge Problem: Definition and Scope

2.1 Formal Grounding

Aumann [1] defines an event E as *common knowledge* among a set of agents N if every agent knows E, every agent knows that every other agent knows E, and so on ad infinitum. Halpern and Moses [2] prove, via the Coordinated Attack problem, that this infinite epistemic tower is *unattainable* between agents communicating over an unreliable channel: no finite exchange of messages can produce common knowledge of coordination.

This impossibility is not a minor technical caveat; it is constitutive. Any system claiming to "solve" CKP is either restricting the reliability assumption (trusted channels), restricting the agent set (closed membership), or claiming less than strict common knowledge under a different name.

Definition 1 (Common-Knowledge Problem, CKP). *The Common-Knowledge Problem is the challenge of maintaining knowledge that would be knowable in principle—if authorised by policy and enabled by availability of communication—where both the authorisation gate and the communication channel are governed by whichever entity or rule-based protocol the participating community has chosen to trust.*

Definition 1 carries three analytically distinct components. The *epistemic ceiling*—"knowable in principle"—names the reachable approximation beneath the Halpern–Moses wall. The *policy gate*—authorisation—embeds the governance question inside the definition: what is knowable depends on who controls what may be known. The *physical gate*—communication availability—acknowledges that eclipse attacks, network partitions, and denial-of-service reduce the reachable ceiling further.

2.2 The Trustless Illusion

A common claim in the blockchain literature is that distributed ledgers solve CKP "without trust." This claim is technically false; the honest formulation is *trust-minimised*. Residual trust always remains in: the hardness of the underlying cryptographic assumptions (currently vulnerable to sufficiently powerful quantum adversaries); the honesty of a majority of the validator or miner set; the correctness of client software that almost every participant uses without independent verification; and—most consequentially—the social layer that resolves disputes about which fork represents the "canonical" chain. Naming and governing each trust residual is the first act of CKP governance.

2.3 The Legitimacy Principle

We adopt a responsibility-grounded account of governance legitimacy rather than a normative-ideal account. *Whoever bears the responsibility and liability for a system holds the right to govern it.* A corporation's owner governs the corporate ledger; a ministry answerable to a legislature governs a national registry. This right is bounded by one structural fact: where a system's records bind parties who bear the consequences but did not delegate the governing authority and cannot exit, the owner's governing right and the affected parties' stake diverge. That divergence is the precise trigger condition for trust-minimisation; where it is absent, centralised authority is not merely acceptable but optimal.

3 Related Work

The governance of distributed ledger systems has attracted growing scholarly attention across computer science, law, and organisational theory, though the literature remains fragmented by disciplinary boundaries.

Buterin [32] proposed a taxonomy of blockchain governance along the axis of on-chain versus off-chain rule-change mechanisms, noting that "the question is how to make those changes happen" without making them "arbitrary." Zargham and colleagues [33] formalised DAO governance as a control-theoretic problem, identifying the principal-agent gap between token-holders and protocol developers as the primary instability. De Filippi and Wright [34] examined the tension between "lex cryptographia" and "lex informatica" in the tradition that Lessig [30] initiated, arguing that code governance is ultimately subordinated to the social and legal contexts in which it is embedded.

The empirical blockchain-governance literature has documented concentration systematically. Srinivasan and Lee [29] introduced the Nakamoto coefficient as a measure of minimum entities needed to compromise a subsystem. Messias et al. [38] measured voting-power concentration across major DAOs, finding that the top ten token-holders control 44–58% of votes and that proposals reach majority with an average of 2.84 participating addresses in Compound and Uniswap.

Within political philosophy, the application of canonical governance theory to digital systems has been largely confined to normative arguments for or against specific forms. Lessig [30] warned that code functions as law and should therefore be subject to constitutional constraints. Werbach [35] applied the trust-in-institutions literature to blockchain design. None of this literature, however, provides a systematic ontological model that maps the full canon of political-philosophy archetypes onto CKP systems, derives their decay vectors, and produces an applied diagnostic procedure. That gap motivates the present work.

Closer in spirit to our approach is the political-economy work of Atzori [36], who argued that blockchain governance instantiates forms of political authority that require constitutional analysis, and of Reijers and colleagues [37], who applied virtue ethics and deliberative democracy theory to smart contract governance. We depart from both by adopting a non-normative, decay-first framing: the question is not which governance form is *ideal* but which form's predicted decay is least likely to destroy the CKP guarantee under a given threat model.

4 The Layered Ontological Model

A persistent error in cyber-governance discourse is the conflation of the *consensus mechanism* with the *governance structure*. A proof-of-work chain controlled by three mining pools and a centralised database controlled by a three-member committee are governed *identically*—by an oligarchy—despite opposite consensus mechanisms. To dissolve this conflation we propose a five-layer model in which each stratum is analytically separable, with its own trust assumptions, failure modes, and relevant governance instruments.

4.1 Layer Definitions

L0 – Substrate. The cryptographic primitives, hardware, and network fabric on which all higher layers depend. Trust residuals here include computational hardness assumptions (e.g. discrete-logarithm hardness, lattice hardness under quantum attack), hardware supply-chain integrity, and the reachability of network paths. Eclipse attacks [28] and BGP hijacking operate at L0.

L1 – Consensus. The protocol by which distributed replicas agree on the ordering and validity of state transitions: Nakamoto proof-of-work, proof-of-stake, Byzantine Fault Tolerance variants (PBFT, Tendermint), or the single-writer authority of a traditional database. The relevant trust assumption is a threshold: the fraction of the validator set that may behave arbitrarily without violating the protocol's safety or liveness guarantees.

L2 – Ledger / State. The shared, tamper-evident record itself: the sequence of committed blocks, the current world-state, and the finality rule that determines when a state transition is irreversible. The finality rule is a critical interface: who is allowed to declare a state *final* is a governance question masquerading as a technical one.

L3 – Rule-Governance. The procedures by which the rules themselves are changed: the upgrade path, the key-management policy, the emergency-response authority, and the amendment process. This is the stratum at which political governance primarily operates. The upgrade key, the emergency multisig, and the pause function are instruments of L3 power.

L4 – Social / Legitimacy. The human community—developers, validators, users, regulators, courts— whose collective interpretation of the protocol determines which fork is "real," which upgrade is legitimate, and whether a disputed state transition will be honoured by downstream actors. The Ethereum community's July 2016 decision to hard-fork in response to the DAO hack [40] is a pure L4 act: no L1 mechanism changed; the social layer declared a new canonical chain.

4.2 The Governance Locus

A critical structural observation follows directly from the layer model: *decentralisation at L1 provides no protection against capture at L3.* A protocol can exhibit a Nakamoto coefficient of twenty at the consensus layer while its upgrade process is controlled by a single maintainer organisation. The political analysis must therefore target L3 and L4 primarily, with L0–L2 treated as the technical substrate that sets the *feasibility boundary* for governance choices at the higher layers.

4.3 The Capability Constraint: Sybil-Resistance

One mechanism occupies a position between the technical and political strata. Sybil-resistance—the capacity to distinguish genuine participants from multi-

plied fake identities—is a trust-management tool whose *presence or absence* determines which L3 governance forms are even representable. Douceur [27] proved that without a logically centralised authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity. Without a proof-of-personhood mechanism, "weight by head" is not merely unwise; it is *unrepresentable*: the system can only weight by resource (stake or hashpower), and any nominal "democracy" collapses into a resource-weighted plutocracy.

This is not a normative constraint but a *feasibility-determining capability*: it sets the feasible set of governance forms that L3 can express.

5 Eight Governance Archetypes

Each archetype is a canonical point in the design space of L3 governance. We characterise each by: its *principle of legitimacy*; its grounding in primary political-philosophy sources; at least one *historical case* of its operation and decay; at least one *modern digital-governance case* that tests whether the predicted decay re-instantiates; its characteristic *decay vector*; and the conditions under which it is the *correct* choice for a CKP system.

5.1 Archetype I: Autocracy

Principle of legitimacy. A single will, vested by necessity or capacity, is the only guarantor of order; responsibility is total, so the governing right is total.

Primary sources. Hobbes's *Leviathan* [3] grounds autocracy in the rational calculus of self-preservation: in the state of nature, life is "solitary, poor, nasty, brutish, and short," and the social covenant transfers all coercive power to the sovereign in exchange for peace. Sovereignty, for Hobbes, is *indivisible*: divided sovereignty is no sovereignty. Bodin [4] added that sovereignty is *absolute and perpetual* (*la puissance absolue et perp'etuelle*) and that the sovereign answers to God alone. Machiavelli [5] reframed legitimacy around effective control: the prince who maintains order is legitimate by consequence, not by antecedent right.

Historical case: Stalinist record falsification. The canonical Common-Knowledge attack under autocracy is the systematic alteration of the official record by the sovereign to whom the record is entrusted. David King's *The Commissar Vanishes* [41] documents Stalin's photographic falsification programme: fallen officials—Nikolai Yezhov, Leon Trotsky, Lev Kamenev—were airbrushed from official photographs and encyclopaedia entries after their executions or exile. In the most precisely documented case, subscribers to the *Great Soviet Encyclopaedia* were mailed instructions in early 1954 to excise pages 21–24 of Volume 5 (the Beria entry) "with scissors or blade" and replace them with extended entries on the Bering Sea and Bishop Berkeley [42]. This is not a pathology of a corrupt autocracy; it is the *structural implication* of a governance model in which a single authority controls both the record and the record of the record.

Modern case: Single-key blockchain control. Any permissioned ledger or bridge protocol governed by a threshold of 1-of-1 or 2-of-3 co-located signers instantiates autocracy at L3. The Axie Infinity Ronin Bridge hack of March 2022 exploited a validator set of nine keys of which four were controlled by a single organisation, reducing the effective threshold to control over those four keys [49]. The structural failure is identical to Stalin's: a single authority controlled both the record and the mechanism of its revision.

Decay vector. The absence of a check on the watchman (*quis custodiet ipsos custodes*, Juvenal [21]) means the decay path is not gradual but binary: the system functions until the principal becomes an adversary, at which point it fails completely and irreversibly with respect to the CKP guarantee.

Correct choice. Autocracy is the correct CKP governance when: the threat model explicitly excludes the sovereign as adversary; the records do not bind non-consenting parties; exit is available at negligible cost; and speed and administrative simplicity outweigh the risk of principal corruption. This describes most intra-organisational record-keeping systems correctly.

5.2 Archetype II: Technocracy / Epistocracy

Principle of legitimacy. Knowledge confers the right to govern; those who understand the domain most deeply will make decisions of highest quality, and the governed benefit from deferring to that expertise.

Primary sources. Plato's *Republic* [6], Books V–VII, constructs the philosopher-king argument: only those who have apprehended the Form of the Good are qualified to rule, and they must be *compelled* into governance precisely because their superior wisdom reveals politics to be an unpleasant necessity. The Platonic programme immediately faces what we term the *selection problem*: to identify the wisest requires wisdom the selector may not possess. Brennan's *Against Democracy* [25] revives epistocracy in contemporary terms, arguing that universal suffrage violates a competence principle and that governance should be restricted to those who demonstrate informational and analytical competence. The central-bank independence literature (Alesina and Summers [26]) argues by analogy: democratic monetary policy suffers from time-inconsistency bias, and delegation to technical experts produces better outcomes.

Historical case: The Chinese imperial examination. The *keju* examination system (c. 605–1905 CE) is the longest-running technocratic experiment in recorded history. Initially designed to recruit administrators on merit—competence in Confucian scholarship, administrative law, and literary composition—it decayed in two parallel processes. First, exam content ossified into the Eight-Legged Essay (*bagu wen*), measuring calligraphic conformity rather than admin-

istrative capacity. Second, differential access to tutors converted nominal meritocracy into hereditary advantage: the *shenshi* gentry class reproduced its position across generations, transforming an open competition into a closed guild. Plato's selection problem manifests here as a credential-capture problem: whoever controls the definition of "knowledge" controls who governs.

Modern case: Protocol maintainers and certificate authorities. Bitcoin Core's governance is a technocracy: a small set of maintainers with commit rights—approximately five individuals at any given time—determine what software the network runs. Their legitimacy derives from demonstrated cryptographic and systems expertise, peer recognition, and a long track record. The CA/Browser Forum presents a more adversarially tested case. When Andrew Ayer's monitoring of Certificate Transparency logs revealed that Symantec had issued over one hundred test certificates for domains it did not control, Google Chrome engineers—acting as a competing technocratic authority —unilaterally distrust Symantec across a three-year transition [47]. DigiNotar was distrusted within 72 hours of the discovery of over 500 rogue certificates in 2011 [47]. The system functioned because an external monitor possessed both the technical capacity to detect the failure and the market power (browser inclusion) to enforce a sanction.

Decay vector. Technocracy decays via credential capture (the guild closes its membership criteria around the incumbents) and via the laundering of value judgements as technical facts. The selection problem is never fully solved: the process by which experts are identified and retained is itself a political act, and one that is systematically invisible in epistocratic self-presentation. In open-source governance, the more common decay is *burnout-induced concentration*: the maintainer set shrinks because the work is uncompensated and adversarial, amplifying the power of whoever remains.

Correct choice. Technocracy is appropriate when the domain is genuinely technical, the cost of error is catastrophic, the expert set is accountable through a meta-mechanism (browser vendors can defect; the kernel community can fork), and the governed community has cheap exit.

5.3 Archetype III: Meritocracy

Principle of legitimacy. Power is allocated by demonstrated merit on a continuous, measurable scale: productivity, hashpower, stake, reputation.

Primary sources. A critical primary source demands attention: Michael Young coined the term "meritocracy" in his 1958 satirical dystopia *The Rise of the Meritocracy* [18] as a *pejorative*. The narrative ends in popular revolt against a hardened meritocratic elite. In his 2001 *Guardian* op-ed Young wrote: "It is good

sense to appoint individual people to jobs on their merit. It is the opposite when those who are judged to have merit of a particular kind harden into a new social class without room in it for others." Hayek [19], in Chapter 6 of *The Constitution of Liberty*, distinguishes *merit* (deserved by effort and virtue) from *market value* (determined by scarcity and demand), warning that conflating them provides a spurious moral justification for unequal outcomes that are in fact the product of luck and circumstance.

Historical case: The Venetian Serrata. The Great Council of Venice was initially a meritocratic body of leading families distinguished by commercial success and civic contribution. In 1297, Doge Pietro Gradenigo's reform—the *Serrata del Maggior Consiglio*—restricted membership to those who had served in the preceding four years or whose patrilineal ancestors had served. The reform was completed and the hereditary principle formalised in the *Libro d'Oro* by 1323 [43]. A meritocratic council became a closed hereditary aristocracy in a single legislative act. The *Serrata* is the template: any merit criterion that is heritable, purchasable, or path-dependent calcifies into aristocracy within a predictable time horizon.

Modern case: Proof-of-work and proof-of-stake as proof of capital. In proof-of-work systems, "merit" is operationally identical to capital expenditure on application-specific integrated circuits (ASICs) and access to cheap electricity. In proof-of-stake, it is identical to holdings of the protocol's native token. Both are purchasable, transferable, and subject to economies of scale that drive concentration: larger pools extract more fees, reinvest more capital, and attract more delegated stake, generating a compounding dynamic with no natural ceiling. The Nakamoto coefficient for Bitcoin mining as of May 2026 stands at approximately 2 (Foundry USA: 34.2% of global hashrate; AntPool: 14.2%; combined: 48.4%) [44]. Where Venice took thirty years to close its books, proof-of-resource networks reach equivalent concentration within eighteen to thirty-six months of launch.

Decay vector. Meritocracy's decay into oligarchy via capital accumulation is not a corruption of the system; it is the equilibrium the system generates. Merit that is purchasable and compounding will concentrate. The Venetian analogy is exact, not illustrative.

Correct choice. Meritocracy is a correct choice only when merit is genuinely non-purchasable, the measurement is regularly re-administered (not heritable or path-dependent), and a Jubilee-style redistribution mechanism prevents compounding. Without all three conditions, the archetype should be classified as *proto-oligarchy* from the outset.

5.4 Archetype IV: Oligarchy / Plutocracy

Principle of legitimacy. Those with the most at stake bear the greatest exposure to system failure; governance rights should therefore be proportional to stake. The *honest* oligarchic claim is that stake-weighted governance aligns incentives with outcomes.

Primary sources. Aristotle's *Politics* [7], Books III and IV, defines oligarchy as rule by the few, specified not by number but by *wealth*: a city with many rich rulers is still an oligarchy; one with few poor rulers is still a democracy. Aristotle's analysis of oligarchic pathology is acute: the wealthy few use governance to protect accumulated wealth rather than to advance the common good, and the formal constitution drifts steadily away from substantive function. Michels [15] supplied the sociological mechanism: *"Who says organisation, says oligarchy."* Any large organisation delegates to leaders; leaders acquire information, time, and skills that ordinary members do not; organisational interest diverges from member interest; the leadership class becomes self-perpetuating. Michels observed this in the German Social Democratic Party—an explicitly egalitarian organisation—and concluded that the iron law admitted no exceptions. Winters [20] modernised the analysis: oligarchy is defined by the *material power of concentrated wealth* and is compatible with any nominal regime type.

Historical case: The late Roman Republic. The Senate of the late Republic (133–27 BCE) presents the fullest historical case of oligarchic decay. The *optimates*—the senatorial aristocracy—converted procedural norms (intercessio, tribunician veto, senatus consultum ultimum) into instruments of wealth defence. The Gracchan reforms, intended to redistribute ager publicus, were blocked and the reformers killed. The Republic ended not through popular revolution but through the oligarchy's own internecine conflict, which it could no longer manage without a military arbiter—the precise Polybian transition to tyranny from above.

Modern case: DAO governance concentration. Messias et al. [38] measured voting-power distribution across Compound and Uniswap governance. The top ten addresses control 57.9% and 44.7% of voting power, respectively; proposals achieve a majority with an average of 2.84 participating addresses. Cong et al. [39] found that the top decile of voters controls 76.2% of voting power in a typical proposal. Lido Finance, as of mid-2025, controlled approximately 24.7% of all staked Ethereum [45]; Coinbase reported 4.5 million ETH staked in Q1 2025 (12.17% of total) [46]. The combined Lido–Coinbase stake exceeds 36%, above the 33% threshold at which a single coordinated actor can block finality in Ethereum's current consensus design. One-token-one-vote governance is *definitionally* plutocracy: one dollar, one vote.

Decay vector. Oligarchy decays through cartelisation—the small group coordinates to extract rents from the majority—and through the 51% attack as its technical analogue: the threshold for consensus capture is not the formal attack threshold of the protocol but the practical coordination threshold of the oligarchs.

Correct choice. Oligarchy is a defensible choice only when: the stakeholders are fully identified, their stakes are non-transferable to anonymous parties, their liability is genuinely bound to their governance power, and exit from the system is sufficiently costly to force voice rather than abandonment. Most token-governed DAOs fail all four conditions simultaneously.

5.5 Archetype V: Direct Democracy

Principle of legitimacy. Self-rule: each affected party has an equal say because all are equally subject to the outcome. Rousseau's *general will* [9] is not the sum of individual preferences but the common interest that each rational agent would identify under conditions of impartiality.

Primary sources. Rousseau [9] argues that sovereignty is inalienable and indivisible: representation is a form of alienation of the will, which he famously dismissed with the remark that the English are free only on election day. Madison, in *Federalist* No. 10 [11], articulated the classical objection: "pure democracies have ever been spectacles of turbulence and contention... and have in general been as short in their lives as they have been violent in their deaths." The majority faction will oppress minorities; representative institutions and spatial scale are the remedy.

Historical case: Athenian democracy. Athenian direct democracy (508–322 BCE) demonstrates every pathology Madison predicted. Demagogues (Cleon, Alcibiades, Hyperbolus) exploited the assembly's susceptibility to rhetorical manipulation. Ostracism, a procedural safeguard against the concentration of personal power, was weaponised as a factional tool and eventually abandoned. The Sicilian Expedition (415–413 BCE), endorsed by the assembly against the cautious counsel of Nicias, ended in catastrophic defeat. The six victorious generals after Arginusae were collectively tried and executed by a mob vote that violated the constitution—the epistemically most extreme form of majority tyranny. Athenian citizenship was, in any case, restricted to adult male citizens: perhaps 30,000–40,000 of a population of 250,000–300,000. "Democracy" was already an oligarchy of the included.

Modern case: The Sybil barrier and the 51% attack. Douceur [27] proved that one-entity-one-vote governance is impossible in a permissionless network without a logically centralised identity authority: any open system is vulnerable

to identity multiplication. The Ethereum Classic 51% attack of January 2019 is the technical form of majority tyranny: an anonymous actor accumulated sufficient hashpower to rewrite 3,693 blocks and execute double-spends worth approximately $1.1 million [48]. Majority rule and the 51% attack are the same act: the protocol *defines* the majority's decision as the valid chain. Low participation further amplifies the pathology: Uniswap governance routinely records turnout below 3% of token supply, meaning motivated minorities capture votes that legally bind the entire system [38].

Decay vector. Absent Sybil-resistance, direct democracy is arithmetically equivalent to plutocracy and exhibits the demagoguery and minority-tyranny pathologies that Madison predicted from majority arithmetic. With Sybil-resistance—proof of personhood [51]—the pathology reduces to voter apathy and capture by organised minorities, which is the contemporary democratic problem in all its familiarity.

Correct choice. Direct democracy is the appropriate archetype only when a robust, at-scale proof-of-personhood mechanism is operational, the stakes of each decision are bounded such that majority tyranny causes recoverable harm, and the participating community is small enough for genuine deliberation to occur.

5.6 Archetype VI: Constitutional Republic

Principle of legitimacy. Legitimacy flows from rules that bind all parties symmetrically, including the rule-makers. No single faction should be able to capture the system; power is divided such that each branch checks the others.

Primary sources. Polybius (*Histories*, Book VI, c. 140 BCE) [8] attributes Rome's exceptional stability to its *mixed constitution*: consuls (monarchic), Senate (aristocratic), and popular assemblies (democratic) each constrain the others, slowing the Polybian cycle. Montesquieu [10] systematised separation of powers as the structural prevention of tyranny. The *Federalist Papers* [12], particularly Federalist No. 51, theorise the necessity of internal constitutional structure: "If men were angels, no government would be necessary." The most penetrating source for the CKP context is Carl Schmitt's *Politische Theologie* [13]: *"Souverän ist, wer über den Ausnahmezustand entscheidet"* ("Sovereign is he who decides on the exception"). No rule-system fully specifies its own emergency response; whoever can suspend the rules is the *de facto* sovereign, regardless of the formal constitution. Schmitt's insight is analytically separable from his subsequent political choices, which are noted but do not invalidate the structural point.

Historical case: Weimar and constitutional erosion. Weimar Germany's Article 48 granted the Reichspräsident emergency decree power subject to legislative veto. Between 1930 and 1933, Chancellor Brüning and subsequently Hitler

governed primarily by decree, normalising the exceptional until the constitutional frame was indistinguishable from the exception. Hitler's appointment as Chancellor was formally constitutional; the *Enabling Act* of March 1933 was passed by a parliament still technically in session. The lesson is not that constitutional systems are fragile; it is that their strength resides in the amendment process and the emergency clause, and those are the targets of any determined captor.

Modern case: The emergency multisig as hidden sovereign. Major DeFi protocols implement a two-layer governance architecture that instantiates the constitutional model: a slow on-chain token vote (the "legislature") and a fast emergency multisig with pause and upgrade authority (the executive with emergency powers). In Compound, the Pause Guardian can disable individual markets without a vote; in Aave, a separate Guardian multisig holds similar prerogatives; in MakerDAO, the Emergency Shutdown Module can be triggered by a threshold of MKR holders. Per Schmitt's analysis, *these multisigs are the true sovereigns of the protocols*, regardless of the token-voting framing. Multiple bridge protocol exploits between 2022 and 2024 validated this architecturally: attackers who compromised the emergency multisig controlled the protocol's assets.

Decay vector. Constitutional systems decay through normalisation of the exception—the Schmittian pathology—and through capture of the amendment process. The amendment process is the key: a constitution is only as strong as the procedure by which it can be changed, and concentrated amendment power converts a constitutional republic into a de facto autocracy with ceremonial trappings.

Correct choice. The constitutional republic is the appropriate archetype for any CKP system that: binds non-consenting parties at significant scale, has a multi-year to multi-decade intended lifespan, and cannot rely on homogeneous trust among participants. It is the most expensive and slowest archetype to build honestly but the only one that contains structural resistance to all eight decay laws simultaneously.

5.7 Archetype VII: Anarchy / Code Is Law

Principle of legitimacy. The code is the only legitimate authority; whatever the protocol permits is legitimate; immutability is the supreme value.

Primary sources. Lessig's *Code and Other Laws of Cyberspace* [30] introduced the phrase "code is law"—as a *warning*, not an endorsement. Lessig's argument is that code is a form of regulation and should therefore be subject to the same constitutional scrutiny as law; the cypherpunk appropriation of the phrase as a

libertarian slogan inverts his meaning. Timothy May's *Crypto Anarchist Manifesto* [31], distributed at CRYPTO '88, articulated the aspiration: "cryptologic methods will fundamentally alter the nature of corporations and of government interference in economic transactions." Hobbes [3] supplies the baseline against which the anarchist position must be evaluated: the state of nature, absent any sovereign, degrades into "the war of all against all." Anarchy generates demand for a sovereign; that demand is the seed of the next autocracy.

Historical case: The Icelandic Commonwealth. The Icelandic Commonwealth (930–1262 CE) is the most sustained historical experiment in institutional anarchy. A system of private law enforcement, clan-based arbitration, and no central executive functioned for approximately three centuries. Its decay—the *Sturlung Era* of civil war (1220–1264) culminating in Norwegian annexation—followed the Hobbesian prediction: concentrated private power (the Sturlungar clan) achieved de facto governance while the formal constitution had no mechanism to check it. Anarchy produced an autocracy by the time the social cost had become intolerable.

Modern case: The DAO hack and the Ethereum fork. On 17 June 2016, an attacker exploited a reentrancy vulnerability in The DAO's Solidity code and drained 3.6 million ETH (then valued at approximately $70 million) [40]. The attacker's action was a *valid execution* of the deployed bytecode; under the "code is law" doctrine, the funds belonged to the attacker. On 20 July 2016, at block 1,920,000, the Ethereum community executed a hard fork, crediting the drained funds to a recovery contract and stranding the attacker's gains. Ethereum Classic is the chain maintained by those who refused to fork and therefore held to "code is law." This incident is the definitive empirical refutation of code-as-governance: immutability is not a property of the code but a *social choice not to fork*. The L4 sovereign—the community of validators, exchanges, developers, and users who decided which chain was "Ethereum"—overrode the L1 consensus of Ethereum Classic on the question of legitimacy, if not on the question of hashpower.

Decay vector. Anarchy is not a stable equilibrium; it generates demand for a sovereign that fills the governance vacuum. The DAO fork created a named sovereign (the Ethereum Foundation and the broad developer/validator community) where the original design had denied one. Ethereum Classic subsequently suffered three documented 51% attacks (2019–2020), demonstrating that a small chain without an implicit social sovereign is precisely as secure as its hashrate.

Correct choice. "Code is law" is acceptable as the *default* layer—the baseline behaviour absent social-layer intervention—but never as the *only* layer. The emergency exception is always present; the only question is whether it is acknowledged and governed or left unnamed and therefore ungovernable.

5.8 Archetype VIII: Bureaucratic Administration

Principle of legitimacy. Rational-legal authority: rules are applied impersonally and predictably by technically trained officials selected on objective criteria. The office, not the person, holds the power.

Primary sources. Weber [14] identified bureaucracy as the institutional form of rational-legal authority and the most technically efficient form of organisation ever developed. Its virtues—precision, speed, formal equality, continuity, discretion, subordination to authority—come at the cost of what Weber called the *stahlhartes Gehäuse*: the iron cage of procedural rationality in which formal rules crowd out substantive judgment. Merton [16] documented the pathological form: bureaucratic ritualism, in which officials treat procedural compliance as an end in itself rather than as a means to the organisation's purpose. Niskanen [17] modelled bureaucratic budget-maximisation: agents who control information about costs have incentives to expand their operations regardless of the social value of the output.

Historical case: The Chinese imperial bureaucracy in decline. The Qing-dynasty bureaucracy of the nineteenth century represents the terminal state of Weberian decay applied to a system that had once been technically superior to its contemporaries. The eight-legged essay format had by this period become entirely self-referential: examining calligraphic conformity to a canonical style rather than any practically applicable knowledge. The bureaucracy's response to the Taiping Rebellion, the Opium Wars, and the pressures of industrialising neighbours was procedurally conformant and substantively incompetent—a precise instantiation of Merton's goal displacement.

Modern case: Change-advisory boards and the CrowdStrike incident. In any production system, the entity that can deploy code to production is the *de facto* sovereign of the system's behaviour—the Weberian rational-legal authority over the technical stack. The CrowdStrike content-configuration update of 19 July 2024 crashed an estimated 8.5 million Windows endpoints globally [50]. The failure mode was pure Merton: a change-management process that satisfied procedural requirements (automated testing, staged rollout protocols) while failing the substantive purpose (ensuring the update was safe). In blockchain governance, the pull-request merge authority of core developers and the key-signing authority of multisig holders are the bureaucratic sovereign, typically undocumented and unaccountable despite holding real power.

Decay vector. Bureaucracy decays into two characteristic pathologies. Goal displacement (Merton): procedure becomes the goal, and substantive competence atrophies. Administrative capture: the professional administrators become their own interest group, using procedural complexity to protect their position.

In the CKP context, the deeper danger is that bureaucratic administration becomes a *shadow sovereign*—the ops team that controls deployment outranks the governance token holder who controls the on-chain vote, and this power differential is invisible in the protocol's self-description.

Correct choice. Bureaucratic administration is unavoidable in any production system with operational complexity; the governance task is to bind it with transparency, rotation, and ex-ante constraints so that administration does not silently become rule.

6 Cross-Cutting Decay Laws

The following laws act on all archetypes simultaneously, not on one in particular. They constitute the dynamic machinery through which any governance form is deformed over time.

6.1 Anacyclosis (Polybius, c. 140 BCE)

Polybius's *anacyclosis* [8] describes a six-stage constitutional cycle: kingship decays into tyranny; tyranny is overthrown by aristocracy; aristocracy decays into oligarchy; oligarchy is overthrown by democracy; democracy decays into mob rule; mob rule collapses into demand for a strongman who initiates the next kingship. The cycle's engine is simple: each good form contains within itself the incentive structure that produces its corrupt twin. Polybius's *solution* was the mixed constitution—setting the forms against each other so that the decay of each is checked by the strength of the others. The application to CKP governance is precise: no governance archetype is stable indefinitely, and the design task is to *instrument against your archetype's known decay*, not to find a form that does not decay.

6.2 The Iron Law of Oligarchy (Michels, 1911)

Michels's iron law [15] holds that every organisation, however democratic in charter, tends toward oligarchy through the structural logic of delegation. Leaders acquire information and skill advantages; the mass of members lacks the time, expertise, or incentive to exercise oversight continuously. This is not a claim about human nature but about organisational dynamics. It should be treated as the *default attractor state* of any CKP governance system: the Nakamoto coefficient will tend downward; the multisig signer set will tend to shrink; the maintainer set will tend to concentrate in one organisation. Decentralisation is not a state one reaches; it is a force one must continuously exert against this attractor.

6.3 The Principal-Agent Problem (*Quis Custodiet?*)

Every act of governance delegation—from stakeholders to validators, from the community to the multisig, from the board to the technical team—creates an agent who possesses private information about their own behaviour and who has incentives that may diverge from the principal's. Juvenal's *quis custodiet ipsos custodes* [21] names the regress: the watcher must be watched, and that watcher also. The formal principal-agent literature (Jensen and Meckling [22]) adds that optimal governance design minimises agency costs through alignment of incentives (compensation, slashing, reputation) and monitoring (transparency, audits, third-party review). In CKP governance the relevant instantiation is: every multisig signer, every validator, and every core developer is an agent with a private key. The security model of the protocol depends on their not defecting.

6.4 Regulatory Capture (Stigler, 1971)

Stigler [23] demonstrated that regulated industries systematically capture their regulators: regulated parties are concentrated, informed, and persistently motivated; the public interest is diffuse, uninformed, and episodically motivated. In CKP governance, the analogous dynamic is *governance capture*: the entities most active in protocol governance are those with the most to gain from governance outcomes—large token-holders, mining pools, and infrastructure providers—and they consistently outparticipate the diffuse mass of ordinary users. The CA/Browser Forum before Certificate Transparency is a clean case: the body designed to govern certificate authority trustworthiness was dominated by the certificate authorities whose trustworthiness it was meant to govern.

6.5 The State of Exception (Schmitt, 1922)

The Schmittian insight [13] is structurally unavoidable: no rule- system specifies its own emergency response completely, because the space of possible emergencies is unbounded. The gap is filled by whoever is authorised—formally or informally—to decide that an emergency exists and to act outside normal procedure. In a CKP system, this is the pause guardian, the emergency multisig, and the "we will hard-fork if needed" capability that the Ethereum developer community demonstrated in 2016. Identifying the holder of exception authority is the most important single diagnostic act in CKP governance, because that entity is the true sovereign regardless of what the formal governance documentation describes.

6.6 The Sybil Constraint (Douceur, 2002)

Douceur's result [27]—that Sybil attacks are always possible in a permissionless setting absent a centralised identity authority—implies that the feasible set of L3 governance forms is contingent on whether identity is solved. Without proof of

personhood, any "democratic" governance reduces to resource- weighted plutocracy in the limit. With a robust proof-of-personhood mechanism, head-weighted forms become representable, though they remain vulnerable to the concentration dynamics of archetypes III and IV as token distributions evolve.

6.7 Concentration Economics and the Nakamoto Coefficient

Economies of scale in mining, staking, and protocol operations push relentlessly toward centralisation. Srinivasan and Lee [29] defined the Nakamoto coefficient as the minimum number of independent entities required to compromise a given subsystem. Empirically, every measured proof-of-work and proof-of-stake network exhibits a Nakamoto coefficient that decreases monotonically after the initial growth phase unless explicit counter-measures are taken. Bitcoin mining (NC ≈ 2 as of May 2026) and Ethereum staking (NC ≈ 3–4) are below the threshold of meaningful decentralisation by any reasonable standard [44,45]. These figures must be monitored continuously and used to trigger governance redesign when they cross operational thresholds.

6.8 Exit, Voice, and Loyalty (Hirschman, 1970)

Hirschman [24] established that members of a declining organisation can *exit* (leave), *voice* (protest internally), or remain in *loyalty*. The balance between exit and voice determines whether governance failure is checked by defection or by reform. The most consequential structural novelty of blockchain governance relative to territorial politics is that *exit is cheap*: forking a protocol is roughly equivalent to the cost of secession in a territorial state, which is catastrophic, but the fork costs its advocates only computational resources and social coordination. This changes the dynamic in two opposing directions. Cheap exit reduces the incentive for voice: disgruntled minorities leave rather than fight. But cheap exit also prevents tyranny from consolidating: a majority that becomes too oppressive will simply haemorrhage users to a fork. Ethereum Classic's survival after 2016 is the empirical test case. This is the single most important structural asymmetry between territorial and digital governance, and the one most frequently ignored in direct applications of political theory to blockchain governance.

7 Synthesis: A Decay-First Analysis Framework

7.1 Thesis, Antithesis, and Synthesis

Thesis. Political philosophy is the primary empirical source for CKP governance because the problem is constitutively about human power, incentive alignment, and the long-run dynamics of authority. The cryptography is solved engineering; the governance is not.

Antithesis. The analogy leaks in four documented directions, and importing political- philosophy intuitions without adjustment produces errors. First,

the cheap-exit property of forking restructures the exit/voice balance in ways that have no clean territorial analogue. Second, the governed "citizens" of a protocol are often pseudonymous capital units rather than persons, making democratic concepts representable only after the Sybil problem is solved. Third, code's literalism—its execution of bytecode exactly as written, regardless of intent—creates failure modes (the DAO reentrancy bug; the Parity multisig freeze) with no analog in legal interpretation. Fourth, the absence of a Weberian monopoly on legitimate violence over a territory means that a protocol's "sovereign" holds power only over actors who choose to run the software.

Synthesis. Political philosophy should be used as a *catalogue of failure modes and decay vectors*, not as a normative menu of desirable regime types. The engineering question is not "which archetype is ideal?" but "given my threat model, which archetype's predicted decay is least likely to destroy the CKP guarantee within my intended operational lifespan?" The historical record, filtered through the eight decay laws, then provides a rich empirical basis for that prediction—not a proof, but a disciplined prior.

7.2 Summary of Archetypes

Table 1 summarises the eight archetypes on the five axes most relevant to CKP governance selection.

Table 1. Summary of the eight governance archetypes. NC = Nakamoto coefficient; "Correct" indicates the minimal conditions for appropriate use.

Archetype	**Legitimacy source**	**Decay vector**	**Modern analogue**	**NC threat**
Autocracy	Single will	Record falsification	Single-key bridge	NC = 1
Technocracy	Expert knowledge	Credential capture	Core developers	NC $\approx$ 5
Meritocracy	Measurable merit	Capital compounding	PoW / PoS pools	NC $\to$ 2
Oligarchy	Stake proportion	Cartelisation	DAO top 10	NC $\approx$ 2–3
Direct democracy	Head count	Sybil / apathy	Token voting	NC = voters
Constitutional	Bounded rules	Exception capture	Multisig guardian	NC varies
Anarchy	Code alone	Social-layer override	"Code is law"	N/A
Bureaucracy	Rational-legal	Goal displacement	Ops / CAB	NC = ops team

8 Applied Diagnostic Method

The ontology produces a six-step procedure for practitioners designing or auditing a CKP governance structure.

Step 1: Specify the threat model. Enumerate the adversary classes in priority order: rational profit-seekers (manageable through incentive alignment), coercive state-level adversaries (manageable only through geographic and jurisdictional distribution), and the principal itself (resolvable only through trust-minimisation at L3 and L4). Every downstream governance choice is a function of this specification. Where the principal is not in the threat set and the records bind only consenting parties, centralised administration with strong audit logging is the correct choice. Where the principal is in the threat set—as in any system where records bind parties who cannot exit—trust-minimisation at L3 is not optional.

Step 2: Name the sovereign. Locate the fastest path by which the system's history could be altered against a participant's will. Ask: who holds the upgrade key; who controls the emergency multisig; who can merge a critical pull request; who can partition the network at L0? That entity is the true sovereign at L3, regardless of what the governance documentation asserts. Publish this analysis. If it cannot be published honestly, the system is an autocracy in fact.

Step 3: Map to an archetype. Locate the current governance structure in the typology of Sect. 5, using the *actual* distribution of L3 power, not the *stated* distribution. Most systems will be found to be in Archetype IV (Oligarchy) or Archetype I (Autocracy) in fact, regardless of their stated archetype.

Step 4: Read the decay row. Take the characteristic decay vector of the identified archetype as a *prior prediction* about how the system will fail. Identify the leading indicators: for oligarchy, the Nakamoto coefficient trend; for technocracy, the size and insularity of the maintainer set; for constitutional republic, the use frequency of the emergency exception.

Step 5: Instrument against the predicted decay. Deploy monitoring and structural countermeasures calibrated to the predicted decay. For oligarchy: publish and alert on the Nakamoto/Gini coefficient for all L3 power dimensions. For the Schmittian exception: impose automatic expiry on emergency powers; require on-chain ratification within a bounded window. For principal-agent drift: implement transparent execution logs, third-party audits, and rotation requirements for keyholders. For concentration economics: impose stake caps or graduated voting-power curves to slow the Venetian Serrata dynamic. For the Sybil constraint: integrate or commission a proof-of-personhood mechanism before claiming any head-weighted governance form.

Step 6: Schedule re-diagnosis. Per anacyclosis, governance is not a state one reaches but a process of continuous decay that requires continuous counterpressure. Schedule a full governance audit at intervals appropriate to the system's rate of change: annually for fast-evolving protocols, every three years for slower- moving institutional systems. Define triggering thresholds—Nakamoto coefficient below k, emergency power invoked more than n times per period,

maintainer set reduced below m organisations—that force an unscheduled re-diagnosis.

9 Discussion: Limitations and Open Problems

9.1 The Limits of the Analogy

We have argued throughout that political philosophy is an empirical source for CKP governance rather than a source of normative templates; the residual worry is that the analogy is persuasive enough to mislead. The cheap-exit asymmetry is the most dangerous gap: political intuitions about the futility or violence of secession systematically overestimate the cost of exit from a protocol, leading practitioners to over-invest in governance mechanisms that are appropriate for captive populations but unnecessary when users can fork. We recommend that practitioners explicitly budget for fork scenarios when evaluating governance investment—a practice with no equivalent in territorial political design.

9.2 Identity as the Unsolved Foundation

The Sybil constraint establishes that the entire space of head-weighted governance forms is contingent on solving identity. Current proof-of-personhood mechanisms (Worldcoin [51], BrightID, Proof of Humanity) have achieved limited coverage at global scale and face genuine tensions between privacy and Sybil-resistance. Until identity is solved at scale, practitioners face a choice between plutocracy (resource-weighted) and autocracy/technocracy (trust-based selection). This is not a failure of governance design; it is a constraint imposed by mathematics.

9.3 The Temporal Problem

A system designed optimally for its initial threat model will be suboptimal as the threat model evolves. Quantum computing threatens L0 cryptographic assumptions and will require protocol-level migration at a scale with no historical precedent. Regulatory environments shift governance feasibility across jurisdictions. The validator population changes demographics, interests, and geography over time. The correct response is not to over-engineer for imagined future threats but to ensure that the amendment process itself remains healthy: a constitutional republic whose amendment process is captured is worse than an honest autocracy with a succession plan.

9.4 Measurement and the Nakamoto Coefficient

The Nakamoto coefficient is an imperfect measurement instrument. Pool membership is volatile; concentration figures vary across trackers and measurement

windows; the coefficient measures *enumerable* entities but not *collusion probability*, which is a function of incentive alignment rather than headcount. We recommend complementing the Nakamoto coefficient with incentive-alignment measures: what fraction of validator revenue would be at risk in a detected collusion event; what is the geographic and jurisdictional distribution of signers; what is the market-cap fraction held by the top ten addresses. No single metric suffices; governance health is multi-dimensional.

10 Conclusion

We have proposed a layered ontological model for the governance of the Common-Knowledge Problem and demonstrated its grounding in both the canonical tradition of political philosophy and the documented empirical record of modern digital governance. The model's central claim is precise: the primary obstacle to maintaining trustworthy shared state over the long run is not cryptographic but *political*, and the most comprehensive empirical library about political failure is the 2,500-year record of how human governance structures succeed, decay, and collapse.

The framework yields three actionable conclusions.

First, the selection of a governance archetype is an engineering decision against a threat model, not a normative aspiration. The correct archetype is the one whose predicted decay is least likely to destroy the CKP guarantee within the intended operational lifespan, given the specific adversary classes in the threat model.

Second, the true sovereign of any CKP system is not the entity named in the governance documentation but the entity identified by the "Find the Sovereign" diagnostic: whoever can alter the record fastest against a participant's will. That entity must be named, published, constrained, and periodically rotated.

Third, governance is not a state one reaches; it is a continuous counter-pressure against the decay forces described in Sect. 6. Designing a governance structure and not re-diagnosing it is equivalent to writing a security policy and not auditing it: the threat model will have moved before the policy is deployed.

The right to fork—cheap exit—is the structural novelty that digital governance contributes to the tradition of political thought. It is both the most powerful anti-tyranny mechanism available and the reason that the Polybian cycle in digital systems does not run to completion: a majority that becomes sufficiently oppressive will simply be forked around. That mechanism must be preserved, documented, and exercised when necessary.

The ontological model proposed here is not complete. The identity problem remains open. The interaction between regulatory law and protocol governance is undertheorised. The dynamics of multi-chain and cross-chain governance introduce game-theoretic complexities not addressed in any single-polity political theory. These are the open problems. What the present framework provides is a disciplined starting point: eight archetypes, eight decay laws, and a six-step

procedure that converts 2,500 years of hard-won political wisdom into an engineering checklist.

References

1. Aumann, R.J.: Agreeing to disagree. The Annals of Statistics 4(6), 1236–1239 (1976)
2. Halpern, J.Y., Moses, Y.: Knowledge and common knowledge in a distributed environment. Journal of the ACM 37(3), 549–587 (1990)
3. Hobbes, T.: Leviathan, or The Matter, Forme and Power of a Common-wealth Ecclesiasticall and Civill. Andrew Crooke, London (1651)
4. Bodin, J.: Les Six livres de la République. Jacques du Puys, Paris (1576)
5. Machiavelli, N.: Il Principe [The Prince]. Antonio Blado, Rome (1532). Written c. 1513
6. Plato: The Republic [Politeia], c. 375 BCE. Trans. G.M.A. Grube, rev. C.D.C. Reeve. Hackett, Indianapolis (1992)
7. Aristotle: Politics [Politika], c. 350 BCE. Trans. C.D.C. Reeve. Hackett, Indianapolis (1998)
8. Polybius: The Histories, Book VI, c. 140 BCE. Trans. R. Waterfield. Oxford University Press, Oxford (2010)
9. Rousseau, J.-J.: Du Contrat Social, ou Principes du droit politique. Marc-Michel Rey, Amsterdam (1762)
10. Montesquieu, C. de S.: De l'esprit des lois. Barrillot & fils, Geneva (1748)
11. Madison, J.: Federalist No. 10: The Union as a Safeguard Against Domestic Faction and Insurrection. In: Hamilton, A., Madison, J., Jay, J.: The Federalist Papers. J. and A. McLean, New York (1788)
12. Madison, J.: Federalist No. 51: The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments. In: Hamilton, A., Madison, J., Jay, J.: The Federalist Papers. J. and A. McLean, New York (1788)
13. Schmitt, C.: Politische Theologie: Vier Kapitel zur Lehre von der Souveränität. Duncker & Humblot, Munich (1922). Trans. G. Schwab as Political Theology. MIT Press, Cambridge MA (1985)
14. Weber, M.: Wirtschaft und Gesellschaft: Grundriß der verstehenden Soziologie. Mohr, Tübingen (1922). Trans. G. Roth and C. Wittich as Economy and Society. University of California Press, Berkeley (1978)
15. Michels, R.: Zur Soziologie des Parteiwesens in der modernen Demokratie. Klinkhardt, Leipzig (1911). Trans. E. and C. Paul as Political Parties. Free Press, New York (1962)
16. Merton, R.K.: Bureaucratic structure and personality. Social Forces 18(4), 560–568 (1940)
17. Niskanen, W.A.: Bureaucracy and Representative Government. Aldine-Atherton, Chicago (1971)
18. Young, M.: The Rise of the Meritocracy 1870–2033: An Essay on Education and Equality. Thames & Hudson, London (1958)
19. Hayek, F.A.: The Constitution of Liberty. University of Chicago Press, Chicago (1960)
20. Winters, J.A.: Oligarchy. Cambridge University Press, Cambridge (2011)
21. Juvenal: Satirae, Satire VI, ll. 347–348, c. 100 CE. Trans. N. Rudd. Oxford University Press, Oxford (1991)

22. Jensen, M.C., Meckling, W.H.: Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics 3(4), 305–360 (1976)
23. Stigler, G.J.: The theory of economic regulation. Bell Journal of Economics and Management Science 2(1), 3–21 (1971)
24. Hirschman, A.O.: Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States. Harvard University Press, Cambridge MA (1970)
25. Brennan, J.: Against Democracy. Princeton University Press, Princeton (2016)
26. Alesina, A., Summers, L.H.: Central bank independence and macroeconomic performance: Some comparative evidence. Journal of Money, Credit and Banking 25(2), 151–162 (1993)
27. Douceur, J.R.: The Sybil attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) Peer-to-Peer Systems. LNCS, vol. 2429, pp. 251–260. Springer, Berlin (2002). https://doi.org/10.1007/3-540-45748-8_24
28. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on Bitcoin's peer-to-peer network. In: Proceedings of USENIX Security 2015, pp. 129–144 (2015)
29. Srinivasan, B.S., Lee, L.: Quantifying decentralization. Blog post, Earn.com (2017). https://news.earn.com/quantifying-decentralization-e39db233c28e
30. Lessig, L.: Code and Other Laws of Cyberspace. Basic Books, New York (1999)
31. May, T.C.: The Crypto Anarchist Manifesto. Distributed at CRYPTO '88 conference, Santa Barbara, CA (1988). https://www.activism.net/cypherpunk/crypto-anarchy.html
32. Buterin, V.: Notes on blockchain governance. Blog post (2017). https://vitalik.eth.limo/general/2017/12/17/voting.html
33. Zargham, M., Zhang, Z., Preciado, V.: A state-space modeling framework for engineering blockchain-enabled economic systems. In: Proceedings of the IEEE Conference on Decision and Control 2019 (2019)
34. De Filippi, P., Wright, A.: Blockchain and the Law: The Rule of Code. Harvard University Press, Cambridge MA (2018)
35. Werbach, K.: The Blockchain and the New Architecture of Trust. MIT Press, Cambridge MA (2018)
36. Atzori, M.: Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation 6(1), 45–62 (2015). https://doi.org/10.22495/jgr_v6_i1_p5
37. Reijers, W., O'Brolcháin, F., Haynes, P.: Governance in blockchain technologies and social contract theories. Ledger 1, 134–151 (2016)
38. Messias, J., et al.: Understanding blockchain governance: Analyzing decentralized voting to amend DeFi smart contracts. In: Proceedings of the 2023 Financial Cryptography and Data Security Conference. arXiv:2305.17655 (2023)
39. Cong, L.W., et al.: Centralized governance in decentralized organizations. Working paper, American Finance Association (2022). https://afajof.org/management/viewp.php?n=157500
40. Mehar, M.I., et al.: Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. Journal of Cases on Information Technology 21(1), 19–32 (2019)
41. King, D.: The Commissar Vanishes: The Falsification of Photographs and Art in Stalin's Russia. Henry Holt, New York (1997)
42. Great Soviet Encyclopaedia, Volume 5 subscriber mailing, early 1954. Documented in: Radio Free Europe / Radio Liberty archives; Reinhardt University History Program, https://blogs.reinhardt.edu/history/
43. Lane, F.C.: Venice: A Maritime Republic. Johns Hopkins University Press, Baltimore (1973)

44. CoinDesk: Bitcoin mining pools with 75% of hashrate back open standard for block construction. CoinDesk (11 May 2026). https://www.coindesk.com/markets/2026/05/11/bitcoin-mining-pools-with-75-of-btc-hashrate-join-open-standard-for-block-construction
45. Lido Finance: Lido Poolside Recap: Tokenholder Update, August 2025. https://blog.lido.fi/recap-lido-q3-2025-tokenholder-update/
46. BitcoinWorld: Coinbase stakes 4.5 million ETH in Q1, maintains self-imposed validator cap (2025). https://bitcoinworld.co.in/coinbase-stakes-4-5-million-eth-q1/
47. SSLMate: Timeline of Certificate Authority Failures. https://sslmate.com/resources/certificate_authority_failures (accessed May 2026)
48. Nesbitt, M.: Deep chain reorganization detected on Ethereum Classic (ETC). Coinbase Security Blog (January 2019). Cited in: The Hacker News, https://thehackernews.com/2019/01/ethereum-double-spend-attack.html
49. CertiK / Chainalysis: Axie Infinity Ronin Bridge hack post-mortem (March 2022). Multiple security-blog sources (2022)
50. Microsoft: Helping our customers through the CrowdStrike outage. The Official Microsoft Blog (20 July 2024). https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/
51. World Foundation: Worldcoin: A decentralized protocol for identity and finance. Technical whitepaper v1.0 (2023). https://whitepaper.world.org/