Journal of Institutional Economics (2026), **22**, e21, 1–15
doi:10.1017/S1744137426100599

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Beyond 'permissionless': governance, commitment, and rule change in public blockchains

Craig Steven Wright

University of Exeter, UK
Email: cw881@exeter.ac.uk

(Received 18 March 2026; revised 30 April 2026; accepted 2 May 2026)

Abstract

The blockchain economics literature often models consensus participants as anonymous, interchangeable agents operating without institutional context. This paper argues that this 'permissionless' assumption describes open admission but abstracts from governance over rule change. Once governance is restored, mutable blockchain systems face a standard commitment problem: rule-changing coalitions may revise protocol rules after participants make chain-specific investments. The paper develops this claim through a comparative-institutional analysis of eight public blockchain systems and two illustrative cases: the BTC Core governance episode and the Ethereum DAO intervention. TCP/IP provides the institutional comparator: technical systems can evolve extensively while preserving base-layer semantic fixedness. Once governance is included, blockchain security is constrained not only by consensus costs but also by institutional commitment conditions: base-layer fixedness, coalition concentration, coordination thresholds, and identity-linked accountability.

Keywords: base-layer fixedness; blockchain; governance; institutions; permissionless consensus

Introduction

A blockchain is a distributed ledger system in which transactions are recorded in blocks and validated according to a shared protocol. Participation in submitting transactions may be open, but the rules governing protocol change are determined through identifiable governance processes.

Recent blockchain economics has produced important formal results about the security limits of open consensus systems. In this literature, participants are typically modelled as anonymous and interchangeable agents who can enter and exit without legal identity, sunk capital, or institutional constraint. Those assumptions are analytically useful, but they also define the scope of the results. They describe a world without governance over rule change. The issue is not that these models are internally wrong, but that their institutional assumptions are narrower than the public-policy and institutional claims sometimes drawn from them.

The contribution of this paper is a single integrated claim. By modelling blockchain systems as 'permissionless', the formal blockchain economics literature treats open admission as though it implied the absence of governance. Once governance over rule change is restored, mutable architectures face a standard commitment problem under discretionary revision: rule-changing coalitions able to alter base-layer rules after participants have made chain-specific investments can change the terms on which those investments were undertaken. The comparative-institutional question is therefore which systems possess credible base-layer fixedness and which do not. Stated more sharply: once governance is

© The Author(s), 2026. Published by Cambridge University Press on behalf of Millennium Economics Ltd. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

Table 1. Governance mechanisms in selected public blockchain systems

Governance mechanism	Mechanism	Systems where operative
1. Repository/ implementation authority	Maintainers or core teams control what changes enter the reference implementation	BTC Core maintainers; Go Ethereum; Solana Labs
2. Foundation or corporate funding	Foundations or firms fund development, roadmap, grants, and ecosystem priorities	Ethereum Foundation; IOHK/ Cardano; Solana Foundation; BNB Chain/Binance
3. Miner or validator concentration	A limited set of pools, validators, or staking providers controls adoption-critical block production	BTC mining pools; Ethereum staking providers; BNB Chain validator set; Solana supermajority validators
4. Development sponsor influence	Firms funding development may influence agenda-setting and protocol direction	Blockstream/BTC Core; ConsenSys/ Ethereum; Block/Spiral grants
5. Fork classification and activation design	Change proponents frame revisions as soft forks, hard forks, client releases, emergency interventions, or token votes, each imposing different coordination burdens	SegWit and block-size dispute; Ethereum hard-fork governance
6. Token-weighted governance	Governance votes are allocated by token holdings, stake, or delegated voting power	MakerDAO; Uniswap; Tezos

included, blockchain security is constrained not only by consensus costs but also by institutional commitment conditions. The formal characterisation of the credibility frontier is in a companion paper.

The question is, therefore, comparative-institutional rather than technological: under what conditions can a protocol commitment be credible? Credibility does not require literal irreversibility. It requires institutional constraints on later discretion, including decision-right dispersion, transparency, reputational exposure, switching costs, and coordination thresholds for rule change. As North (1990) argues, formal rules are effective only when complemented by informal constraints; a formally fixed protocol therefore functions as a commitment device only where accompanying norms of non-revision sustain it.

The argument builds directly on the literature treating blockchain as an institutional technology. Following Hodgson (2006), institutions are the systems of established rules that structure interaction; this is the working definition on which the comparative-institutional analysis rests. Davidson *et al.* (2018) identify blockchain's institutional significance; Frolov (2021) shows that actual blockchain systems are hybrid and governance-laden; Alston *et al.* (2022) show that governance burdens fall on identifiable human actors; and Davidson (2025a, 2025b) shows that crypto-governance does not escape familiar problems of corporate control and concentrated voting. This paper adds a specific mechanism to that literature. Where base-layer rules remain mutable, governance over rule change creates a commitment problem for participants who have made chain-specific investments. An online supplementary appendix accompanies the paper. Part A contains extended case material on the BTC (Bitcoin Core) episode and the Ethereum Decentralized Autonomous Organization (DAO) intervention. Part B contains the fuller Transmission Control Protocol/Internet Protocol (TCP/IP) discussion, expanded source documentation for Table 2, and methodology notes on the eight-system audit.

Williamson's (1979) transaction-cost economics supplies the primary framework. Chain-specific investments create exposure to later opportunism where a rule-changing coalition retains discretion over the base protocol. Kydland and Prescott (1977) clarify the time-consistency problem created by that discretion, while Tirole (1986) provides a supplementary account of information and authority within governance hierarchies. The present paper is diagnostic: it identifies the institutional mechanism and shows why the 'permissionless' assumption narrows the scope of existing formal results. A companion paper formalises the credibility frontier; the present paper establishes the institutional mechanism and comparative evidence motivating that model.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

Table 2. Quantitative governance metrics (illustrative, dated)

System	Concentration metric	Governance form	Source/period
BTC Core	Top-5 mining pools ≈75% hashrate	PoW; concentrated reference-client authority (Bitcoin Core); funded-developer presence (Blockstream, Spiral)	Btc.com; Mempool.space (2023–2024); Crunchbase; Spiral.xyz
Ethereum	Top-3 staking entities ≈33% of staked ETH	PoS; multi-client validator environment (Geth dominant); Foundation treasury ≈USD 1.6B (April 2024)	Beaconcha.in (early 2024); Clientdiversity.org; EF Treasury Report (April 2024)
Solana	Nakamoto coefficient on stake ≈33	PoS; single dominant reference client (Solana Labs); Foundation funding	Solana Beach; Helius Labs (2023–2024); SF grant disclosures
Cardano	Not quantified	PoS; foundation- and IOHK/IOG-led development; many stake pools, single dominant client	Cardano Foundation reports; PoolTool (2023–2024)
BNB Chain	Active validator set = 21	PoS; corporate-led development (Binance-affiliated)	BNB Chain documentation; validator-set disclosures (2023–2024)
Uniswap	Top delegate concentration; specific share not quantified	Token-weighted governance via UNI; identifiable institutional delegates (a16z and others)	Snapshot.org; Tally.xyz; Uniswap forum (2023–2024)
MakerDAO	Routine-poll turnout < 10% of MKR supply	Token-weighted governance via MKR; concentrated holdings among large delegates	vote.makerdao.com; MKRGov.science (2023–2024)
Tezos	Not quantified	On-chain stake-weighted amendment; bakers exercise governance authority	TZ Stats; TzKT amendment history (2023–2024)

Note: Concentration metrics are order-of-magnitude estimates from the public sources cited, accessed across 2023–2024. Shares vary over time and are presented to document the existence of identifiable, non-atomistic governance structures, not stable point estimates. Cardano and Tezos rows are marked 'Not quantified' because effective amendment authority and stake-pool implementation concentration were not summarised as a single metric for this audit; both systems are included as governance-mechanism evidence, with their structural features documented in the Governance form column. The Uniswap concentration cell similarly notes that the precise share held by top delegates is not quantified here. The institutional point – that adoption-critical actors are a small, identifiable set rather than an anonymous mass – is robust to within-period variation in the precise figures. Expanded source documentation for each row, with specific URLs and retrieval dates, is provided in the Online Supplementary Appendix, Part B.

The scope of the 'Permissionless' assumption

This section does not argue that the formal literature is wrong. It identifies the institutional features that are excluded when 'permissionless' is treated as a complete description of the system rather than as a claim about admission.

Origins of the term

The term 'permissionless' does not appear in the Bitcoin whitepaper (Nakamoto, 2008). It became prominent later as blockchain systems were classified into 'permissioned' and 'permissionless' types. In that taxonomy, 'permissioned' systems restrict participation in validation or consensus, while 'permissionless' systems allow open participation subject to the protocol's technical rules. The distinction is useful, but it is taxonomic. It describes access to participation; it does not, by itself, describe the institutional arrangements through which protocol rules are changed.

The distributed-systems literature uses a different framing. Pease *et al.* (1980) and Lamport *et al.* (1982) distinguish processors that follow the protocol from processors that behave arbitrarily. That distinction is exogenous to the model: the analysis asks whether agreement can be reached given a specified distribution of compliant and non-compliant actors. It does not derive compliance from investment, legal identity, reputational exposure, or governance arrangements. When blockchain economics adopts analogous honest/Byzantine or compliant/deviating partitions, the institutional source of those behaviours therefore remains outside the model.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

How the assumption functions in formal models

The assumption appears across several strands of the formal blockchain economics literature. The following review groups ten papers into four categories to show how the assumption functions analytically and which institutional features are placed outside the model.

Category 1: attack-cost models. Budish (2025) derives that the flow cost of maintaining trust scales with the value of transactions secured. The proof treats consensus participants as anonymous agents whose only relevant decision is whether to comply with or attack the protocol, given an exogenous cost structure. Auer (2019) inherits the same framing, modelling proof-of-work mining as a zero-profit activity with no sunk capital and concluding that double-spending attacks are profitable under the model's assumptions.

Category 2: mining-equilibrium models. Biais *et al.* (2019) and Saleh (2021) derive compliance as an equilibrium outcome under explicit assumptions about anonymous, atomistic participants competing in well-defined consensus games. Carlsten *et al.* (2016) similarly treat miners as anonymous agents with no institutional commitments outside the consensus game.

Category 3: permissionless-consensus impossibility results. Budish *et al.* (2024) and Lewis-Pye and Roughgarden (2023) prove impossibility results for permissionless consensus under specific assumptions about agent anonymity and Sybil-resistance. Their results are valid given the formal definition of permissionless they use.

Category 4: currency and settlement models. Schilling and Uhlig (2019) model Bitcoin as a competing currency within a general-equilibrium framework; Chiu and Koeppl (2019) study blockchain-based settlement; Huberman *et al.* (2021) analyse fee dynamics. These models treat protocols as fixed and abstract from rule-change governance.

What the abstraction excludes

Across these strands, the recurring abstraction is the same: participants are modelled as anonymous, interchangeable agents whose compliance or deviation is not explained by governance structure, legal identity, reputational exposure, or chain-specific investment. That abstraction is appropriate for many formal purposes. It becomes limiting when the results are used to characterise public blockchain systems whose rule-changing processes are institutionally organised.

The proofs in these papers are valid given their assumptions. The issue is scope. The formal definition of permissionless – anonymous agents, no identity, no institutional embedding – may not describe the systems the literature models. If the systems contain identifiable actors, sunk investments, foundations, developer-funding relationships, and rule-changing coalitions, then conclusions derived under the formal definition do not necessarily extend to the systems.

The literature points in the opposite direction. Frolov (2021), Alston *et al.* (2022), and Davidson (2025a, 2025b) all show that blockchain systems are governed through identifiable actors, concentrated participation, and institutional arrangements that do not disappear merely because admission is open. Governance over Rule Change develops that point comparatively. The implication for the formal literature reviewed above is not invalidity, but a limited domain: models that abstract from governance cannot, without additional institutional assumptions, explain governance over rule change.

The next section, therefore, asks whether the excluded institutional features are empirically present in the major public blockchain systems under examination.

Governance over rule change

The permissioned/'permissionless' distinction usefully describes admission but is incomplete for analysing real systems. A system can be permissionless at the admission layer while remaining

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

governed at the rule-change layer. The two are independent dimensions, and conflating them obscures the institutional structure of the systems being analysed.

This section builds on the institutional literature by making the governance layer explicit. Davidson *et al*. (2018) treat blockchain as an institutional technology; Frolov (2021) documents hybridity; Alston *et al*. (2022) analyse polycentric governance; Davidson (2025a, 2025b) documents concentration in DAO voting. The present audit contributes a comparative characterisation across eight systems.

The eight systems examined – BTC Core, Ethereum, Solana, Cardano, BNB Chain, Uniswap, MakerDAO, and Tezos – are selected as a purposive sample covering major governance archetypes: proof-of-work, proof-of-stake, foundation-led, corporate-led, and token-governed systems. The sample is illustrative rather than representative. Its purpose is to identify recurring governance mechanisms, not to estimate their distribution across all blockchain systems. Table 1 codes observable mechanisms – such as repository authority, development funding, validator or miner concentration, fork framing, and token voting – rather than measuring normative legitimacy or governance quality. The comparison is diagnostic: it documents the governance layer that the 'permissionless' label omits, not a claim that all systems are governed in the same way.

The selection rule is explicit. The sample includes systems satisfying three criteria: top-twenty layer-1 market capitalisation at the time of analysis (giving operational history sufficient for documented governance episodes); architectural diversity (proof-of-work, multiple proof-of-stake variants, foundation-led, corporate-led, token-governed); and publicly documented governance events permitting institutional analysis. Excluded under these criteria: layer-2 rollups (Arbitrum, Optimism, Polygon), which inherit base-layer governance from host chains; newer architectures with shorter operational histories (Aptos, Sui, Hedera); and systems with overlapping governance archetypes already represented (Avalanche, Polkadot, Cosmos, Algorand). A wider sample would strengthen the documented institutional pattern, not change its existence. Methodology notes on the eight-system audit, including data limitations and what the audit supports and does not support, are provided in the Online Supplementary Appendix, Part B.

The relevant comparison is not governance versus no governance, but the form governance takes. Governance over Rule Change documents the form across the eight-system sample.

Established governance arrangements identify decision-makers and specify the scope of their authority. The blockchain systems examined here exhibit governance arrangements that vary on both dimensions, but in no case is the governance layer absent.

Reference implementations matter because most participants coordinate around a limited number of clients. Maintainers control what changes are merged. Where reference-implementation authority is concentrated, the maintainer set holds effective control over what the protocol becomes.

Foundations and firms influence governance by funding developers, maintaining roadmaps, distributing grants, and coordinating ecosystem priorities. Examples include the Ethereum Foundation, IOHK/Cardano, the Solana Foundation, and BNB Chain/Binance.

Block production and protocol adoption are often concentrated among a limited number of mining pools, validators, or staking providers. Concentration makes rule-change coordination cheaper for the coalition with the adoption-critical share, regardless of formal openness at the admission layer.

Funding relationships are governance-relevant because they affect which developers are supported, which technical priorities are advanced, and which protocol directions are most easily resourced. Sponsor-developer alignment is documented for several of the systems in the sample.

Protocol changes differ in their coordination burden. A change framed as a soft fork, hard fork, client release, emergency intervention, or governance vote imposes different coordination costs on different participants and routes the change through different governance pathways.

Activation design matters because different implementation paths allocate coordination burdens differently across miners, validators, exchanges, and node operators.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

In token-governed systems, formal decision rights are allocated by token holdings, stake, or delegated voting power. The institutional consequence is that voting concentration becomes the relevant governance metric.

Token voting does not remove governance; it relocates governance authority to holders and delegates whose identity is sometimes pseudonymous, sometimes publicly identified.

A common objection is that non-mining nodes constrain developers by refusing unwanted software. This describes a backstop, not a governance mechanism. Most users defer to maintainers, exchanges, and large operators.

Governance is not measured by the number of persons running software. It concerns decision rights, resource concentration, and the practical capacity to effect or block rule changes.

Base-layer fixedness as a commitment device

Governance over Rule Change established that public blockchain systems contain identifiable governance layers. This section explains why that matters. Where participants make chain-specific investments, governance over base-layer rule change creates a commitment problem. The comparison with TCP/IP is instructive because TCP/IP shows how technical systems can evolve extensively while preserving base-layer semantic fixedness. The institutional issue is not whether innovation occurs, but where it occurs: above a stable base layer, or through discretionary revision of the base layer itself.

The TCP/IP structural parallel

TCP/IP provides the clearest comparator because it combines open participation with stable base-layer rules, and supports decades of higher-layer innovation without revising the base.

TCP/IP is not ordinarily analysed using the 'permissionless' framing. It performs a technical function within an institutional environment: ISPs, telecommunications law, contract, commercial regulation, professional norms, and court systems supply the institutions outside the protocol. The protocol is embedded; it does not stand alone.

The critical shared property is base-layer semantic fixedness. TCP achieves this through a design pattern: a stable wire format and connection state machine specified in RFC 793, with reserved option fields and unused header bits left available for future extension. New transport-layer features (Hypertext Transfer Protocol (HTTP)/3 over QUIC, Transport Layer Security (TLS), congestion-control extensions) are introduced as either separate protocols or optional features at the extension points provided. The base protocol does not change; the application and feature layers do.

This technical structure matters institutionally. No ordinary participant can unilaterally alter the base layer; doing so would require coordination across millions of independent operators using multiple competing implementations. The base layer is therefore set in stone in the institutional sense relevant here: stable enough that economic actors plan, invest, and contract on the assumption that the rules will not be revised under their feet.

Bitcoin was described in equivalent commitment terms by its author: 'The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime' (Nakamoto, BitcoinTalk Post #126, 2010). Like TCP/IP, Bitcoin's base layer was intended to provide stable consensus rules and ledger semantics on which higher-layer applications could be built. SegWit is an example of a base-layer transaction-format change adopted after deployment – demonstrating that Bitcoin's implementation in practice differs from this design intent.

The claim of base-layer fixedness for TCP/IP requires distinguishing two kinds of change. RFC 793 (Postel, 1981) specified the core wire format, the connection state machine, and the semantic rules of the protocol, and reserved option fields and unused header bits for future extension. Subsequent RFCs commonly cited – RFC 1122, 3168, 6093, 6528, 7323 – populate reserved fields, clarify ambiguous behaviour, or specify optional features at extension points the original specification provided for. None of them modifies the base wire format or the core state machine. A TCP implementation conforming to

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

RFC 793 from the early 1980s still interoperates with the modern Internet. Filling a reserved field that the original specification anticipated is not a revision of the base protocol; it is the use the original specification was designed to permit. The institutional pathway through which extensions are introduced – the Internet Engineering Task Force (IETF) standards process, multi-vendor interoperability requirements, and the absence of any coalition with discretionary rule-changing authority over the deployed network – is what disciplines extension to remain wire-compatible with the installed base. That institutional pathway, operating on a base layer whose core semantics have not been revised since 1981, is what the paper means by base-layer fixedness.

The institutional analogy is therefore precise. TCP/IP, HTTP, SMTP, and DNS demonstrate that digital infrastructure can support extensive innovation while preserving base-layer semantic stability. When base-layer rules are credibly resistant to unilateral revision, investment migrates to higher layers rather than being consumed by struggles over the transport base. Protocols retaining discretionary governance at the base layer force participants to price the risk of post-investment rule change into every chain-specific commitment. In Williamsonian terms, stable lower-layer rules reduce the risk of ex post discretionary revision.

Table 3 summarises the comparison.

Commitment and governance: a Williamsonian core with extensions

The TCP/IP comparison identifies the institutional mechanism: base-layer fixedness enables investment by participants whose returns depend on the rules being stable. The same mechanism applies to blockchain systems, where participants make chain-specific investments under expectations about the rules.

The claim is conditional. Where investment is specific to a protocol and rule-changing discretion is held by an identifiable coalition, the standard Williamsonian hold-up problem applies. The first condition is documented empirically; the second is documented by the audit in Governance over Rule Change.

This clarifies the Davidson *et al.* (2018) claim that blockchains control opportunism through cryptographic enforcement. Cryptographic enforcement controls opportunism only against the rules currently encoded. Where rule-changing discretion exists, the rule-changing coalition can revise the rules being enforced; cryptography enforces whatever the new rules are.

Two institutional conditions follow. First, base-layer rules must be resistant to discretionary revision after investment – base-layer fixedness, in the paper's terminology. Second, the actors holding rule-changing authority must bear consequences for opportunistic revision – identity-linked transparency.

Operationalising base-layer fixedness. Stability is a credibility property, but the underlying institutional inputs are observable. Five correlates are informative. First, the coordination threshold for a base-layer rule change: how many miners, validators, foundations, exchanges, or token holders must align before a change becomes effective. Second, the concentration of the implementation pathway: whether one reference client controls the upgrade route, or multiple independent clients must each adopt and ship a change. Third, the identity-linkage of the rule-changing actors: whether maintainers, foundations, or validators bear personal legal, professional, or commercial consequences for revisions. Fourth, the historical record of base-layer revisions: a protocol that has revised semantics under coalition action signals future revision is in the choice set; one that has not signals that it is not. Fifth, the credibility of exit: whether a minority can retain meaningful network value after a contested fork.

These correlates do not collapse base-layer fixedness into a single index; they identify the dimensions on which a comparative-institutional study can rank systems. Governance over Rule Change documents the first three across the eight-system sample. The fourth and fifth are illustrated by the BTC Core and Ethereum DAO cases.

A scope qualification on identity-linked transparency. Identifiability raises R, and therefore strengthens commitment, on the specific institutional question this paper addresses: governance over base-layer rule change in systems where participants have made chain-specific investments.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

Table 3. Structural comparison: TCP/IP and Bitcoin as designed

Dimension	TCP/IP	Bitcoin (as designed)
Admission	Broad participation	Open transaction submission
Rules	Public RFC standards; semantically stable base	Public protocol specification; originally set-in-stone design
Operators	ISPs and infrastructure providers; identifiable firms	Miners and service providers; identifiable firms
Legal context	Operates within telecoms, contract, and commercial law	Operates within financial, property, and commercial law
Value proposition	Packet routing	Payment processing
What fixedness enables	Investment in applications and infrastructure above the base layer	Investment in payment infrastructure and applications above the base layer
Analytical framing	Treated as infrastructure within law	Often analysed as if it must substitute for institutional trust The comparison establishes the central institutional distinction used in the rest of the section: technical evolution above a stable base layer differs from discretionary governance over the base-layer rules themselves. An extended treatment of the TCP/IP comparator, including the reserved-fields-versus-base-revision distinction, the institutional pathway by which TCP/IP evolves, and Bitcoin's original commitment language, is provided in the Online Supplementary Appendix, Part B.

Anonymity may be welfare-improving on other margins – censorship resistance, political dissent, financial privacy, surveillance protection. The two margins can be in tension: a system credibly committed through identity-linkage may also be more legible to authorities seeking to compel rule change against identifiable governance actors. The trade-off is real and is not resolved here.

Hold-up. Williamson identifies asset specificity as the critical condition under which governance structure matters. In the property-rights account of Grossman and Hart (1986), where contracts are incomplete, residual control over the asset determines who can appropriate the quasi-rents once investment is sunk. Blockchain participants make four kinds of specific investment: physical asset specificity (mining hardware), site specificity (facilities co-located with low-cost power), human-capital specificity (protocol-specific development expertise), and dedicated-asset specificity (capital committed to platform-specific business activity). Each form is non-redeployable to alternative uses; each generates the rents the rule-changing coalition can capture through opportunistic revision.

The mechanism is general. Participants make investments specific to a protocol; those investments rely on expected protocol rules; rule-changing discretion held by an identifiable coalition creates exposure to post-investment revision; the exposure is the institutional cost the protocol structure imposes on participants. The five-step structure is invariant; the operationalisation varies by architecture.

This is the blockchain version of Williamson's fundamental transformation: ex ante competition among possible systems becomes ex post dependence on the governance coalition controlling the rule environment in which the investment is already sunk. Williamson's framework is inherently comparative. Base-layer fixedness is not universally optimal. It trades reduced opportunism against reduced adaptability. In environments where the central problem is design uncertainty, flexibility may be valuable. In environments where the central problem is post-investment rule discretion, fixedness becomes valuable as commitment. The question is not whether change is good or bad in the abstract. The question is whether the governance structure is aligned with the transaction being governed.

In proof-of-work systems with concentrated reference-implementation authority – BTC Core is the canonical case – the coalition is the maintainer set with commit authority over the canonical client, together with mining-pool operators controlling adoption-critical hashrate. K is low because the coalition is small; hold-up exposure is high because participants have made physical-asset specific investments (ASIC hardware, mining facilities).

In proof-of-stake systems with concentrated staking infrastructure – Ethereum and Solana are illustrative – the coalition extends to staking providers and validator operators alongside reference-implementation maintainers. K is the cost of aligning a heterogeneous validator set against the upgrade signalled by the dominant client. Hold-up exposure shifts toward stakeholder principal and reputational capital rather than physical asset specificity.

In foundation-led architectures – Cardano, Solana, BNB Chain – the coalition is led by a legal entity holding treasury, employment, and roadmap authority over developers and ecosystem partners. K is internalised within an organisational hierarchy. R is high relative to pseudonymous-developer arrangements because the foundation has legal personality and exposure to regulatory action.

In token-governed protocols – MakerDAO, Uniswap, Tezos – the coalition is the set of token holders who turn out to vote, weighted by holdings or delegation. K is mechanically lower because votes can be aggregated atomically through on-chain voting; hold-up exposure for non-voting holders is correspondingly high, since a sufficient quorum can revise governance over the holdings of those who do not participate. The Compound Finance July 2024 incident documented in Davidson (2025b) is the empirical illustration. The relevant institutional question is whether token-governance thresholds, delegation patterns, and turnout produce a coalition that is in practice smaller and more identifiable than the formal voting population suggests.

What is invariant across the four forms is the institutional structure: participants make protocol-specific investments under one expected rule set; a coalition with discretion over base-layer rules emerges; post-investment revision is constrained, if at all, by coordination cost K, identity-linked

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

consequence R, and credibility of exit. What varies is coalition composition and the operational form of K and R.

The object of commitment is base-layer rule stability – the consensus rules, issuance schedule, and ledger semantics – not every application outcome. The relevant discretionary actor is the rule-changing coalition, the set of actors with the practical power to revise base-layer rules and have the revision adopted: maintainers, foundations, large mining or staking entities, dominant token holders, or some combination, varying by architecture.

Time inconsistency. Kydland and Prescott show that discretionary policy is costly when agents are forward-looking. The blockchain analogue is direct: a protocol whose rules can be revised in response to specific outcomes faces the same time-inconsistency problem. Participants who anticipate discretionary revision discount their investment in protocol-specific assets accordingly. Rogoff (1985) extends this, showing that the optimal arrangement is a binding degree of commitment rather than full discretion. A protocol with credible base-layer fixedness operates as a rule rather than a discretionary policy, in the sense formalised by Woodford (2003), where commitment to a policy rule governs the expectations of forward-looking agents.

Hierarchical collusion. Tirole's hierarchy model supplies a secondary mechanism. Where one group holds technical information that other principals cannot easily verify, that group can capture decision authority over the technical agenda. In blockchain governance, maintainers set and dominant client teams hold technical information about implementation pathways, activation logic, and consensus rules that token holders, users, or even foundations may not be able to verify independently. The institutional implication is that technical authority can translate into governance authority in the absence of independent verification.

The BTC Core case study

The BTC Core episode illustrates how the general mechanism operates in a mutable protocol. The case is presented as an illustration of the institutional mechanism, not as proof of capture; the four-product mapping below is treated as a structured hypothesis.

The case is reconstructed from public protocol records, BIPs, repository history, corporate disclosures, public filings, and the contemporaneous block-size dispute and SegWit activation records.

Sponsor alignment. Blockstream, founded in 2014, raised substantial venture funding and developed products commercially complementary to a constrained base layer with off-chain settlement (Liquid sidechain, Lightning infrastructure). Several BTC Core maintainers received Blockstream salary or grants during the SegWit period; Block (formerly Square) funded contributors through its Spiral subsidiary. The institutional fact is the funding flow; the contested claim is the causal effect of the funding on protocol decisions.

Protocol change and activation design. BIP141, Segregated Witness (Lombrozo et al., 2015), activated in August 2017 as a soft fork. It restructured transaction-format encoding, separating witness data from the transaction body. The activation pathway was framed as a soft-fork upgrade; the institutional fact is that the base-layer transaction format was modified through a coordination process the maintainer set effectively controlled.

Three claims should be separated. Governance concentration is well supported by the institutional record. Sponsor-developer incentive alignment is well supported by the funding record. Causal attribution from sponsor influence to specific protocol decisions remains contested and is not settled by the case material.

Economic consequences. After SegWit and retention of constrained base-layer capacity, the system experienced periods of elevated mempool congestion and high fees during demand spikes. Lightning Network adoption proceeded; on-chain payment use cases shifted towards higher-value transactions. The proximate causal decomposition is contested – demand growth, market cycles, and technical constraints all contributed – but the institutional pattern is observable: rule-change choices that

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

retained constrained base-layer capacity coincided with consequences favourable to off-chain alternatives the principal sponsor firms had developed commercially.

Exit and chain split. Forking provides an ex post governance mechanism. Participants who reject a rule change can coordinate on a continuation chain. The block-size dispute produced multiple such forks. The institutional point is not that exit is impossible, but that exit is costly: forks fragment liquidity, infrastructure, and developer attention, and the cost is borne by participants who exit rather than by the rule-changing coalition.

The episode is consistent with a Stigler-Peltzman style capture mechanism. Development funding from firms with commercial complementarity to constrained base-layer capacity (Blockstream, Spiral) flowed to developers controlling the implementation pathway; the activation choices preserved constrained base-layer capacity in directions favourable to off-chain alternatives the funding firms had developed; the institutional pattern is observable even where the specific causal claim remains contested.

The institutional reading can be specified through Stigler (1971) and Peltzman (1976) on the four products that the regulatory authority can supply; Becker (1976) observes, in the same regulatory-capture literature, that regulations surviving the competition for votes tend to be relatively efficient means of redistributing resources. The mapping below is presented as a structured hypothesis consistent with the observed institutional structure, not as a finding that capture occurred. Each product is operationally identifiable in the case material; whether the rule-changing coalition actually exercised them to extract sponsor-aligned outcomes is the contested causal claim that the case material does not settle.

First, direct subsidy. In the BTC Core context, this corresponds to financial transfers from sponsor firms to development teams implementing the relevant changes. Blockstream's funding of multiple BTC Core contributors during the SegWit period and Square/Block's grants through Spiral are documented from corporate disclosures. The funding flow is an institutional fact; the second-order causal effect on protocol decisions is contested.

Second, control over entry. The analogue is control over what enters the canonical reference implementation: which BIPs are merged, which are rejected, which are deferred. Repository-merge authority performs the function of an entry barrier for protocol-direction proposals. Whether this authority was exercised in a sponsor-aligned manner is the contested claim; that the authority existed and was exercised is uncontested.

Third, the regulator's effect on prices, supplies, and treatment of substitutes and complements. In the BTC Core context, the analogue is the rule-changing coalition's ability to alter the relative cost of on-chain settlement versus off-chain alternatives. By retaining constrained base-layer capacity and adopting SegWit as the activation pathway, the protocol changed the relative price of the substitute (on-chain transactions) and the complement (Lightning Network and associated payment-channel infrastructure). The coalition controlled a lever directly analogous to a regulator's price-and-supply lever and exercised it in a direction that systematically advantaged the complement over the substitute.

Fourth, administered scarcity. Conventional regulation can ration access to a scarce resource through licence allocation or quotas. The BTC Core analogue is the deliberate retention of constrained base-layer transaction capacity through the block-size limit. The constraint was not the only technically feasible path in 2017; alternative implementations supporting larger blocks were technically feasible. The choice to retain constrained capacity, framed as a scaling-philosophy decision, produced an administered-scarcity outcome whose distributional consequences fell on transactors who had invested on the basis of expectations about throughput.

The four Stigler products are each individually identifiable in the BTC Core episode. The case does not establish the joint causal claim that the coalition exercised these powers because of sponsor capture rather than independently-held technical convictions; that claim requires evidence the case does not supply. The narrower claim the four-product mapping does supply is institutionally decisive: a mutable governance layer over a system with concentrated implementation authority and identifiable

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

sponsor relationships produces all four products as outputs available to the coalition. The four-product mapping is therefore best read as a hypothesis-generating framework. It identifies the institutional levers available; it does not establish that the levers were pulled with capture-aligned intent. The narrower architectural claim – that a mutable governance layer makes all four levers available to the rule-changing coalition – is what this paper supports. An extended treatment of the BTC Core episode – expanded sponsor-alignment documentation, the four Stigler products developed individually, the technical counterargument in extended form, and the Ethereum DAO mappings against Williamson, Kydland-Prescott, and Tirole – is provided in the Online Supplementary Appendix, Part A.

A technical counterargument deserves an explicit statement. SegWit addressed transaction malleability, an obstacle to second-layer protocols. The technical claim is independent of the institutional one. The institutional reading does not deny technical motivations; it observes that the activation pathway preserved constrained base-layer capacity in a manner consistent with the four-product framework, whatever the proximate technical justification.

The Ethereum DAO intervention

The BTC Core case shows the commitment problem through gradual governance change. The Ethereum DAO episode shows it in acute form: a single crisis forced an explicit choice between base-layer finality and discretionary intervention.

In June 2016, the DAO – a crowdsourced investment vehicle on Ethereum – was exploited through a contract vulnerability, and approximately $60 million worth of Ether was diverted. Because the funds were time-locked, the community had time to coordinate a response. In July 2016, Ethereum adopted a hard fork that altered the ledger state to return the funds to DAO investors. Participants who rejected the intervention continued on Ethereum Classic. The institutional fact is that a settled on-chain outcome was reversed through discretionary base-layer coordination.

A non-intervention rule would have imposed an immediate and visible loss on DAO investors. Discretionary intervention avoided that loss, but at the cost of weakening the general expectation of finality. That is the institutional trade-off: the rule that maximises commitment value over repeated interaction may require refusing the discretionary correction that appears optimal in a particular crisis. The fuller institutional reading of the DAO intervention – mapping the case against Williamson, Kydland-Prescott, and Tirole – is provided in the Online Supplementary Appendix, Part A.

Implications

For blockchain economics

The first implication concerns scope. Formal blockchain economics models derived under anonymous-agent, open-entry assumptions remain valid within those assumptions. Their domain of application is narrower, where public blockchain systems contain identifiable governance actors, sunk investments, and rule-changing coalitions. The implication is extension, not rejection: governance over rule change must be modelled as part of the system rather than treated as external.

Once governance is restored, protocol stability becomes visible as a commitment device. Security is no longer only a function of anonymous entry, attack cost, and consensus incentives; it depends also on identifiable operators, sunk capital, legal and reputational exposure, coordination thresholds, and the rule-changing coalition's capacity to revise.

The formal implication is straightforward. Attack profitability and rule-change incentives should include institutional terms: capital at risk, legal exposure, reputational loss, coordination costs, and the distribution of rule-changing authority. These terms may not eliminate profitable attacks, but they change the comparative statics. A model that sets them to zero describes a different institutional environment from the one documented in Governance over Rule Change.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

For institutional economics

For institutional economics, public blockchain systems provide a comparative field setting for studying commitment devices in technical infrastructure. The design choice between base-layer fixedness and mutable governance is a rules-versus-discretion problem in the sense of Kydland and Prescott, and a discriminating-alignment problem in the sense of Williamson. The BTC Core and Ethereum DAO cases illustrate the costs of discretionary rule change; TCP/IP illustrates the investment-enabling properties of stable base-layer semantics combined with higher-layer innovation.

This clarifies the paper's relationship to the literature. Davidson *et al.* (2018) treat blockchain as an institutional technology; Frolov (2021) shows that actual blockchain systems are hybrid and governance-laden; Alston *et al.* (2022) analyse blockchain networks as polycentric orders; Davidson (2025a, 2025b) shows that crypto-governance reproduces familiar problems of corporate control and concentrated voting. The present paper adds the architectural mechanism, where base-layer rules are mutable, cryptographic enforcement does not by itself control opportunism, because the rule-changing coalition can revise the rules being enforced.

The TCP/IP comparison adds a broader institutional point. Digital infrastructure can evolve through higher-layer innovation while preserving stable base-layer semantics. Blockchain systems that adopt that architecture should support stronger relationship-specific investment because the base rule set is less exposed to discretionary revision. Systems that retain base-layer discretion recreate the Williamsonian problem: participants must price the risk that rules governing their sunk investment may later be revised.

For policy

The policy implication is not that all blockchain systems should be regulated identically. It is that regulatory analysis should distinguish open admission from governance over rule change. The relevant policy variables are institutional: who can revise the rules, how that authority is constrained, whether conflicts are disclosed, and what costs rule changes impose on participants with sunk investments.

First, 'permissionless' should not be used as a complete analytical primitive in regulatory design. Open admission does not imply absence of governance. A system in which anyone can submit transactions may still have concentrated rule-change authority. Regulation that treats such a system as institutionally empty will misclassify the relevant risks. Berg et al. (2020) predict that blockchain will flatten hierarchy and narrow the rationale for much economic regulation; the governance layer documented here points the other way, as identifiable rule-changing authority persists rather than dissolves.

Second, protocol governance is a policy variable. Whether base-layer rules are fixed, mutable, or subject to emergency override affects the incentive environment for participants. Fixity reduces discretionary hold-up but limits error correction; mutability preserves adaptability but creates post-investment rule-change risk. Tulip Trading Ltd. v Bitcoin Association for BSV [2023] EWCA Civ 83 treated as arguable the claim that developers exercising control over network software could owe duties in relation to users' property interests. The institutional significance, on the framework developed here, is that, where developers possess practical rule-changing authority, legal systems may ask whether that authority carries obligations.

Third, sponsor influence over protocol development is a candidate for disclosure rather than prohibition. Where firms fund developers, maintain reference implementations, or sponsor infrastructure that benefits from particular protocol choices, those relationships are governance-relevant. Disclosure requirements would impose compliance costs, but they may be justified where sponsor influence affects rule-change authority over systems in which users and firms have sunk investments.

Fourth, the analysis extends beyond public blockchains. Central Bank Digital Currency (CBDCs), regulated stablecoins, payment networks, and other programmable settlement systems face the same

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

institutional design question: which rules should be fixed at the base layer, which should be revisable, and who should possess revision authority?

Limitations. The paper does not deliver a full equilibrium model of blockchain governance under endogenous rule change; the formal characterisation is in a companion paper. It does not claim causal identification; the case studies illustrate institutional possibility, not causal proof. The eight-system sample is purposive; the documented institutional pattern would be strengthened, not changed in kind, by extension. Quantitative metrics in Governance over Rule Change are order-of-magnitude estimates; the institutional claim relies on the existence of identifiable governance structures rather than stable point estimates. These limitations bound the contribution to institutional diagnosis and comparative analysis.

Conclusion

The central result is that 'permissionless' admission and governance over rule change are distinct institutional dimensions. A blockchain may be open to transaction submission while remaining governed by identifiable actors who control implementation, activation, funding, validation, or token-weighted rule revision. Treating open admission as the absence of governance narrows the institutional scope of formal blockchain economics models.

The comparative audit shows that the systems differ in architecture, but none lack a governance layer. That finding does not invalidate anonymous-agent models; it identifies their domain. Such models describe systems in which governance, legal identity, sunk investment, and rule-changing authority are outside the model. The major public blockchain systems examined here do not fully satisfy that description.

Once governance is restored, base-layer fixedness becomes visible as a commitment device. Where participants make chain-specific investments, discretionary rule-changing authority creates the Williamsonian problem: investors act under one expected rule set, but after investment is sunk, the rule-changing coalition may alter the terms. The BTC Core and Ethereum DAO cases illustrate different margins of that problem – gradual rule change through implementation governance, and acute discretionary reversal of a settled ledger outcome.

The paper's implication is therefore limited but substantive. Existing formal results remain valid under their assumptions, but those assumptions should not be mistaken for a complete institutional description of public blockchain systems. If governance over base-layer rule change is present, then commitment depends on institutional constraints: fixedness of the base rules, dispersion or accountability of rule-changing authority, and coordination costs of revision. The contribution is diagnostic. It identifies the governance layer that the 'permissionless' label obscures and explains why that layer matters for commitment once investment is sunk.

Supplementary material. The supplementary material for this article can be found at https://doi.org/10.1017/S1744137426100599.

References

Alston E., Law W., Murtazashvili I. and Weiss M. (2022). Blockchain networks as constitutional and competitive polycentric orders. *Journal of Institutional Economics* **18**(5), 707–723. https://doi.org/10.1017/S174413742100093X.

Auer R. (2019). Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies. *BIS Working Papers, no. 765.*

Becker G.S. (1976). Toward a more general theory of regulation: Comment. *Journal of Law and Economics* **19**(2), 245–248. https://doi.org/10.1086/466867.

Berg C., Davidson S. and Potts J. (2020). Capitalism after Satoshi: Blockchains, dehierarchicalisation, innovation policy, and the regulatory state. *Journal of Entrepreneurship and Public Policy* **9**(2), 152–164. https://doi.org/10.1108/JEPP-03-2019-0012.

Biais B., Bisière C., Bouvard M. and Casamatta C. (2019). The blockchain folk theorem. *Review of Financial Studies* **32**(5), 1662–1715. https://doi.org/10.1093/rfs/hhy095.

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press

Budish E. (2025). Trust at scale: The economic limits of cryptocurrencies and blockchains. *Quarterly Journal of Economics* **140**(1), 1–62. https://doi.org/10.1093/qje/qjae033.
Budish E., Lewis-Pye A. and Roughgarden T. (2024). The economic limits of permissionless consensus. *Proceedings of the 25th ACM Conference on Economics and Computation (EC '24)* 704–731. https://doi.org/10.1145/3670865.3673548.
Carlsten M., Harry Kalodner S.M.W. and Narayanan A. (2016). On the instability of bitcoin without the block reward. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* 154–167. https://doi.org/10.1145/2976749.2978408.
Chiu J. and Koeppl T.V. (2019). Blockchain-based settlement for asset trading. *Review of Financial Studies* **32**(5), 1716–1753. https://doi.org/10.1093/rfs/hhy122.
Davidson S., De Filippi P. and Potts J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics* **14**(4), 639–658. https://doi.org/10.1017/S1744137417000200.
Davidson S. (2025a). Corporate governance in a crypto-world. *Regulation & Governance* **19**(3), 777–788. https://doi.org/10.1111/rego.12661.
Davidson S. (2025b). The nature of the decentralised autonomous organisation. *Journal of Institutional Economics* **21**, e5. https://doi.org/10.1017/S1744137424000341.
Frolov D. (2021). Blockchain and institutional complexity: An extended institutional approach. *Journal of Institutional Economics* **17**(1), 21–36. https://doi.org/10.1017/S1744137420000272.
Grossman S.J. and Hart O.D. (1986). The costs and benefits of ownership: A theory of vertical and lateral integration. *Journal of Political Economy* **94**(4), 691–719. https://doi.org/10.1086/261404.
Hodgson G.M. (2006). What are institutions? *Journal of Economic Issues* **40**(1), 1–25. https://doi.org/10.1080/00213624.2006.11506879.
Huberman G., Leshno J.D. and Moallemi C. (2021). Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *Review of Economic Studies* **88**(6), 3011–3040. https://doi.org/10.1093/restud/rdab014.
Kydland F.E. and Prescott E.C. (1977). Rules rather than discretion: The inconsistency of optimal plans. *Journal of Political Economy* **85**(3), 473–491. https://doi.org/10.1086/260580.
Lamport L., Shostak R., and Pease M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems* **4**(3), 382–401. https://doi.org/10.1145/357172.357176.
Lewis-Pye A. and Roughgarden T. (2023). Permissionless consensus, arXiv Preprint arXiv: 2304.14701.
Lombrozo E., Lau J. and Wuille P. (2015). BIP. 141: Segregated witness (Consensus layer). *Bitcoin Improvement Proposal*. Available at https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki.
Nakamoto S. (2008). Bitcoin: A peer-to-peer electronic cash system.
North D.C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.
Pease M., Shostak R. and Lamport L. (1980). Reaching agreement in the presence of faults. *Journal of the ACM* **27**(2), 228–234. https://doi.org/10.1145/322186.322188.
Peltzman S. (1976). Toward a more general theory of regulation. *Journal of Law and Economics* **19**(2), 211–240. https://doi.org/10.1086/466865.
Postel J. (1981). Transmission control protocol. *RFC. 793. Internet Engineering Task Force*. https://doi.org/10.17487/RFC0793.
Rogoff K. (1985). The optimal degree of commitment to an intermediate monetary target. *Quarterly Journal of Economics* **100**(4), 1169–1189. https://doi.org/10.2307/1885679.
Saleh F. (2021). Blockchain without waste: Proof-of-stake. *Review of Financial Studies* **34**(3), 1156–1190. https://doi.org/10.1093/rfs/hhaa075.
Schilling L. and Uhlig H. (2019). Some simple bitcoin economics. *Journal of Monetary Economics* **106**, 16–26. https://doi.org/10.1016/j.jmoneco.2019.07.002.
Stigler G.J. (1971). The theory of economic regulation. *Bell Journal of Economics and Management Science* **2**(1), 3–21. https://doi.org/10.2307/3003160.
Tirole J. (1986). Hierarchies and bureaucracies: On the role of collusion in organizations. *Journal of Law, Economics, and Organization* **2**(2), 181–214. https://doi.org/10.1093/oxfordjournals.jleo.a036907.
Tulip Trading Ltd. v Bitcoin Association for BSV. (2023). *EWCA Civ 83. Court of Appeal of England and Wales*.
Williamson O.E. (1979). Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics* **22**(2), 233–261. https://doi.org/10.1086/466942.
Woodford M. (2003). *Interest and Prices: Foundations of a Theory of Monetary Policy*. Princeton: Princeton University Press.

Cite this article: Wright CS (2026). Beyond 'permissionless': governance, commitment, and rule change in public blockchains. *Journal of Institutional Economics* **22**, e21, 1–15. https://doi.org/10.1017/S1744137426100599

https://doi.org/10.1017/S1744137426100599 Published online by Cambridge University Press