BIS

BIS Bulletin

No 126

Blockchain consensus mechanisms and fragmentation

Daniel Eidan, Jon Frost, Rudraksh Kansal, Ulf Lewrick, Sang Hyuk Lim and Tomasz Rybarczyk

6 July 2026

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the BIS or its member central banks. The authors thank Matteo Aquilina, Sebastian Doerr, Pablo Hernández de Cos, Hyun Song Shin and Leanne Zhang for helpful comments and suggestions, and Nicola Faessler for administrative support.

The editors of the BIS Bulletin series are Gaston Gelos and Frank Smets.

This publication is available on the BIS website (www.bis.org).

ISSN: 2708-0420 (online)
ISBN: 978-92-9259-964-5 (online)

Daniel Eidan daniel.eidan@bis.org
Jon Frost jon.frost@bis.org
Rudraksh Kansal rudraksh.kansal@bis.org
Ulf Lewrick ulf.lewrick@bis.org
Sang Hyuk Lim sanghyuk.lim@bis.org
Tomasz Rybarczyk tomasz.rybarczyk@bis.org

Blockchain consensus mechanisms and fragmentation

Key takeaways

- *While all permissionless blockchains use token-based incentives to sustain honest validation, differences in how validator rewards, coordination and participation are structured lead to distinct equilibria and trade-offs between decentralisation, security and scalability.*
- *These trade-offs underpin the emergence of multiple layer 1 networks and the expansion of layer 2 solutions, resulting in fragmentation of infrastructure, liquidity and assets across and within chains.*
- *Tools to mitigate fragmentation – eg bridges and native multi-chain issuance – can reduce frictions, but they reintroduce new dependencies on trust, governance and operational resilience.*

Public permissionless blockchains reduce reliance on centralised intermediaries by using decentralised, open infrastructure. Since the emergence of Bitcoin and Ethereum, activity built on distributed ledger technology (DLT) has expanded rapidly, spanning payments, decentralised finance and broader digital asset markets. Yet rather than converging on a single scalable infrastructure, a multitude of networks have arisen, fragmenting liquidity and diluting network effects. This Bulletin describes consensus mechanisms, asks why fragmentation occurs and explores what it means for market structure and resilience.

We examine how consensus mechanisms in permissionless blockchains balance decentralisation, security and scalability.[1] These choices shape validator participation, costs and coordination and generate distinct equilibria across different layer 1 (L1) blockchains. They have also driven the growth of layer 2 (L2) solutions that execute off-chain. L1s are the base networks that validate, process and finalise transactions directly in the shared ledger (on-chain). L2s, in turn, run on top of an L1 to enhance efficiency and scalability. We assess how this architecture fragments activity across and within chains, and how mitigation tools reduce frictions while introducing new trust, governance and operational dependencies. We conclude with implications for the potential role of permissionless blockchains as financial market infrastructures and for policy. The online appendix provides further details and a glossary.

Consensus mechanisms: equilibria and trade-offs

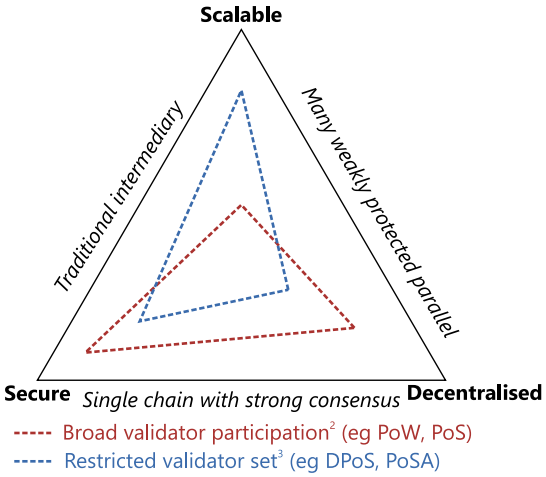
Blockchains are append-only, shared databases (ledgers) maintained by validators who may not know or trust one another. In permissionless settings, anyone may attempt to validate or propose blocks; thus, incentives must align validators' private rewards with the public good of a coherent ledger (eg Budish (2025); Saleh (2021)). Participation depends on chain-specific requirements such as energy

[1] Permissionless blockchains rely on so-called consensus, with incentives in the form of tokens, to align participants whose identities are hidden behind an address (pseudonym). Anyone with the required software can participate without prior approval. Permissioned blockchains use approved (known) validators and established governance. The latter thus resemble governance structures in the traditional financial system, prioritising scalability and security over decentralisation (Bains (2025)).

expenditure (work), minimum "locked" resources (stake), hardware capacity and voting or participation costs (eg fees for attestations or votes).

To sustain an honest equilibrium, validators must be compensated not only for operating costs but also for coordination risks arising from relying on other validators' participation. For example, Bitcoin miners incur energy and hardware costs to earn block rewards (proof of work). Ethereum validators must lock up their native token (Ether) and risk "slashing" penalties (loss of staked tokens) for deviating from predetermined rules (proof of stake). These and other incentives shape validator behaviour and determine whether consensus is maintained. Overly large sets of validators raise coordination costs, while excessive concentration increases the risk of disruption or control (Auer et al (2025)). Seen through this economic lens, blockchain consensus mechanisms are best understood as a range of token-incentivised equilibria (supported by "tokenomics"), in which validator behaviour depends on how rewards, penalties and participation costs are structured.

The trilemma associated with achieving consensus[1] Graph 1



[1] Triangle positions represent general tendencies of consensus mechanisms. The triangle's exact shape and placement may vary by blockchain implementation and configuration. [2] Proof of work (PoW) and proof of stake (PoS) support broad validator participation and thus decentralisation but can introduce scalability constraints in layer 1 networks. [3] Delegated proof of stake (DPoS) and proof of staked authority (PoSA) rely on smaller validator sets, which can enhance coordination efficiency and speed, but reflect different assumptions about validator participation and governance (see Table 1).

Sources: BIS (2022), Buterin (2021); authors' elaboration.

The "blockchain trilemma" highlights the trade-offs between decentralisation, security and scalability (Buterin (2021)). Consensus mechanisms position themselves differently along these dimensions (Graph 1). Allowing many validators to independently verify and confirm blocks supports decentralisation and security, but it also increases communication and verification costs. This limits throughput and raises latency (ie the time needed to confirm transactions), as in proof of work and proof of stake blockchains (red triangle). By contrast, designs that prioritise scalability achieve higher throughput and lower latency confirmations by reducing the number of validators or increasing hardware requirements, which narrows participation and weakens decentralisation, as in delegated proof of stake (eg Tron) or proof of staked authority (eg BNB Smart Chain) (blue triangle). These design choices reflect different economic equilibria rather than purely technical constraints.

Security considerations reinforce these trade-offs. When the value secured by a blockchain increases, the resources required to compromise the network – the attack cost – must also rise to deter malicious behaviour. In permissionless blockchains, these costs are borne by users through fees, congestion rents or dilution of tokens, implying that higher security standards come with tighter capacity constraints.

L1 networks feature distinct consensus mechanisms, shaping cost, latency and resilience (ie the ability to recover from disruptions). Their coexistence reflects competition among platforms to attract users with

diverse needs and preferences. Early blockchains such as Bitcoin and Ethereum prioritised decentralisation and security through broad validator participation. This approach limits scalability: when demand for scarce block space rises, congestion intensifies and transaction fees increase, pushing out more price-sensitive users (Boissay et al (2022); Shin (2026)). Proof-of-stake systems can also face scalability constraints when security relies on large validator sets and frequent coordination. In response, newer L1s feature greater degrees of centralisation, such as smaller validator sets or higher hardware requirements, to raise throughput while lowering latency and fees (Table 1; Table A.1 in the online appendix).

No one size fits all: the plethora of layer 1 consensus mechanisms Table 1

Design [example]	**Consensus mechanism**	**Trade-offs**
Proof of work (PoW) [eg Bitcoin]	Participants expend computing power to add blocks by competing to solve cryptographic puzzles. The protocol adjusts difficulty to maintain steady block times as computing power changes.	Robust and decentralised, but throughput is intentionally low; energy consumption depends on hardware efficiency.
Proof of stake (PoS) [eg Ethereum]	Participants lock up (stake) native tokens and are selected to propose/verify blocks; misbehaviour such as proposing conflicting blocks or failing to attest as required can result in part of the stake being forfeited (slashing). Finality is achieved through many stakers attesting to the same block.	More efficient than PoW and supports rollups for scale, but still faces challenges to decentralisation, due to stake concentration risks, and coordination, due to consensus requiring a supermajority, which can also face scalability constraints.
Time ordering + BFT [eg Solana (PoH + PoS/Tower BFT)]	A cryptographic clock orders events, enabling faster agreement, followed by Byzantine fault tolerance (BFT), in which a supermajority of validators must agree before blocks are confirmed.	Low latency and high throughput, but hardware and bandwidth needs raise barriers to entry for validators, potentially limiting decentralisation.
Probabilistic sampling [eg Avalanche (Snow*)]	Nodes repeatedly poll small, random subsets of validators until the network converges, achieving fast finality with high probability.	Fast confirmation and flexible subnets, but security and liveness depend on sampling settings and the distribution of stake in the network.
Delegated validator sets [eg Tron (DPoS), BNB Smart Chain (PoSA)]	A small, elected or rotating group of validators produces blocks, with selection based on votes or delegated stake.	High throughput and quick finality but concentrates governance and validation power, which may reduce decentralisation.

BFT = Byzantine fault tolerance (a class of consensus methods that allow the system to function correctly even if some validators are faulty or malicious); PoH = proof of history (a cryptographic time source used to create a verifiable and consistent ordering of events); PoSA = proof of staked authority (a small, governance-approved validator set is selected based on a combination of stake and authority); Snow = Avalanche "Snow" family of probabilistic sampling protocols (eg Snowball, Snowman, which achieve consensus through repeated random sampling of small validator subsets); DPoS = delegated proof of stake (token holders delegate their stake to elect a limited, rotating set of validators who produce blocks on their behalf).

Source: authors' elaboration.

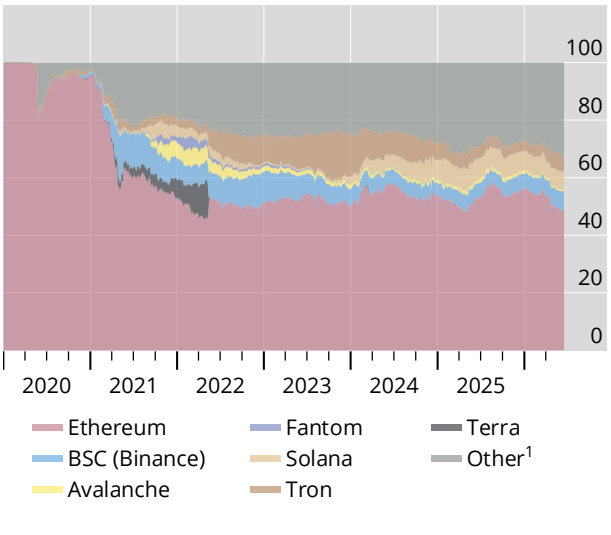
The diversity of networks separates users and liquidity across different, siloed networks. While Ethereum remains dominant in decentralised finance (DeFi), new L1s have expanded "horizontally" (Graph 2.A). Some have disappeared, eg Terra – which grew rapidly before failing spectacularly in 2022 – or have seen falling use, eg Fantom. Meanwhile, some networks have shifted towards modular architectures that split functions "vertically" across layers, providing separation of execution, settlement, data availability and sequencing across specialised layers (Graph 2.B). While specific design features vary (see Table A.2 in the online appendix), all L2 solutions work by processing transactions off-chain and

writing results back to their base L1 for settlement and data availability.[2] This modularity raises efficiency when systems are robust and governance is clear. But it also creates distinct execution environments, each with its own transaction ordering, pricing and points of failure. L2s develop their own liquidity pools and governance mechanisms, adding vertical fragmentation to the patchwork of networks. Modularity thus redistributes, rather than eliminates, trade-offs across layers and introduces new governance and interoperability challenges.

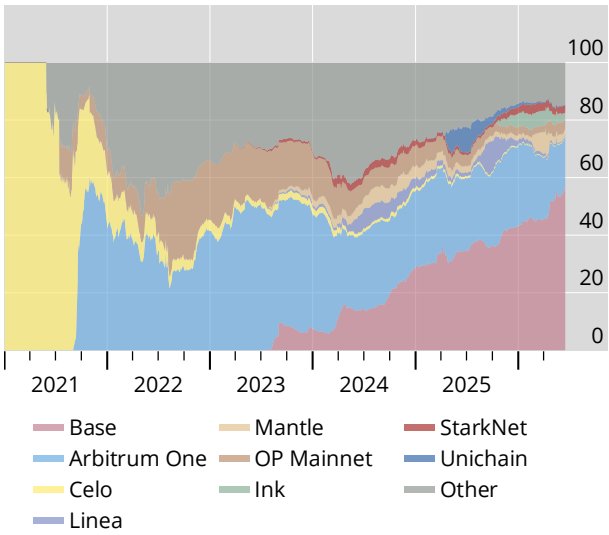
Rising fragmentation across layer 1 (L1) and layer 2 (L2) networks

As a percentage of total value locked — Graph 2

A. Assets and liquidity are fragmented across networks



B. Rising use of L2s points to vertical fragmentation[2]



[1] Also includes L2 networks [2] L2s have been selected based on Token Terminal's methodology

Sources: DefiLlama; Token Terminal; BIS; authors' calculations.

Mitigation mechanisms: benefits and trade-offs

Rising fragmentation across L1 and L2 networks has increased demand for mechanisms to connect assets, liquidity and applications across blockchains. These mitigation mechanisms aim to reduce frictions while preserving basic security and permissionless participation. But none eliminates fragmentation entirely. Instead, each shifts risks based on introducing new trust assumptions, governance arrangements and operational dependencies.

- *Bridges*. Bridges transfer value across blockchains by locking an asset on one network and issuing (minting) a corresponding representation on another. Bridges can be implemented via custodial groups, guardian sets, relayers/oracles or on-chain light-client verification. Bridges are convenient for users, but they concentrate risk: compromised keys, falsified messages and bugs in smart contracts have led to large losses (eg USD 625 million in the March 2022 Ronin Network hack).
- *Native multi-chain issuance*. Large issuers (eg of stablecoins) mint native versions of their tokens across several chains. While these tokens have identical names, they cannot be transferred across

[2] One example of how L2s scale is *rollups*, which batch transactions and post compressed data to the base chain, lowering fees while inheriting L1 security. *Optimistic rollups* assume validity subject to fraud proofs during a challenge window, whereas *zero-knowledge rollups* use validity proofs for faster finality but with greater implementation complexity. Other models include *validiums* (most data are kept off-chain, changing data-availability assumptions), *sidechains* (eg Polygon PoS, which is independent and bridged, but does not inherit L1 security) and *state channels* (eg Lightning Network, which moves repeated interactions off-chain with periodic L1 settlement). Table A.2 in the online appendix gives further details.

chains, and the same user has different wallet addresses on each chain (Graph 3.A). Each version typically trades in its own liquidity pool, deepening fragmentation and reliance on cross-chain arbitrageurs to mitigate price differences. This form of issuance shifts the operational burden from bridges to issuer coordination, treasury management and consistent governance across chains.

- *Shared layers for security, data and sequencing.* Some ecosystems seek to reduce fragmentation in their own environments by providing shared services to multiple rollups. These include shared security, where a common pool of stake backs several L2s; shared data-availability layers that store and publish transaction data so that anyone can verify execution; and shared sequencers that determine transaction ordering across rollups. By coordinating execution and reducing delays, these shared layers can improve efficiency and limit the scope for rents. At the same time, they concentrate governance and operational risk in a small number of components that may become systemically relevant within an ecosystem.

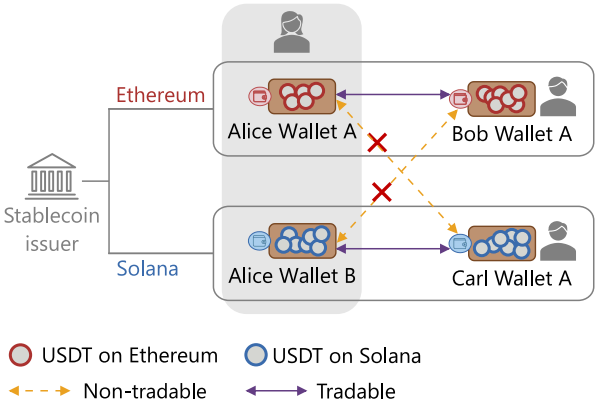
- *Interoperability protocols (message-passing/state coordination).* Rather than moving assets across blockchains, interoperability protocols allow chains to communicate by verified messages or proofs, enabling applications to act remotely (eg mint, redeem, settle). Some systems rely on cryptographic verification, where one blockchain verifies another's state on-chain. Others depend on external parties (eg relayers or oracles) to transmit messages. By keeping assets on their original chains, these designs reduce duplication and fragmentation but introduce new trust assumptions that on-chain verification rather than external intermediaries should minimise.

Rising fragmentation has fuelled rapid growth in the use of interoperability protocols in particular (Graph 3.B). Mitigation mechanisms could reduce some frictions but introduce new dependencies. As private sector experimentation continues, designs that combine verifiable security, transparent governance and clearly defined failure modes are more likely to emerge and to be more robust. At the same time, market participants may converge around a limited number of shared layers, warranting heightened attention to their operational resilience and governance arrangements.

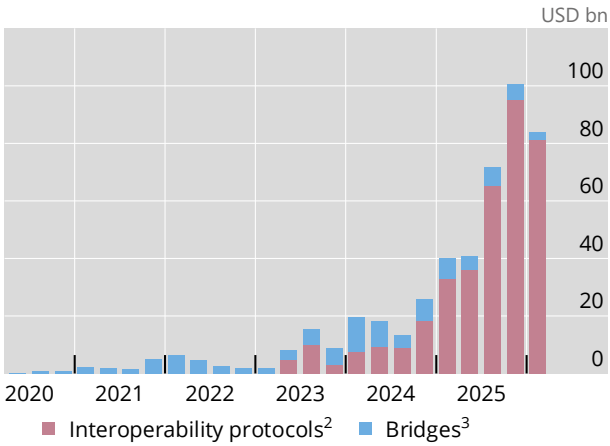
Rising fragmentation has spurred demand for mitigation mechanisms

Graph 3

A. Stablecoin issuers have relied on native multi-chain issuance to access multiple blockchains[1]



B. Use of interoperability protocols has surged



[1] The graph provides a stylised example of how a stablecoin (eg USDT) can be issued natively on multiple blockchains (eg Ethereum and Solana) by the issuer. While this improves availability across blockchains, tokens remain siloed and non-tradable across chains. Wallets are represented with a certain value of tokens (blue or red circles) and wallet address below them. Without mitigation mechanisms, sending stablecoins between wallets on different blockchains (eg Solana to Ethereum) may fail, risking permanent loss. [2] Axelar Network, Circle Cross-Chain Transfer Protocol (CCTP), Chainlink, deBridge, LayerZero. [3] Across, Allbridge Core, deBridge Liquidity Network (DLN), Everclear, Hop Protocol, Hyperbridge, Ren, Stargate, Synapse, zkSync Era Bridge.

Sources: Token Terminal; BIS; authors' elaboration.

The prospect of permissionless blockchains as financial market infrastructures

Permissionless blockchains, including the applications built on them, are intended to provide general purpose financial infrastructure. In practice, however, binding economic constraints drive them towards specialisation and fragmentation. Consensus trade-offs generate multiple equilibria rather than convergence towards a single, unified infrastructure. Mitigation mechanisms designed to reconnect fragmented systems often reintroduce intermediaries and new dependencies. These dynamics limit the extent to which permissionless chains can naturally evolve into financial market infrastructures (FMIs) without additional governance and oversight. If permissionless blockchains are to support functions akin to FMIs, several policy dimensions warrant consideration:

- *Operational and cyber resilience*. Diverse consensus mechanisms, validator incentives and governance models complicate risk assessment, incident response and recovery planning. While consolidation around common middleware can reduce fragmentation, it may create critical points of failure if a small number of shared services become critical to system functioning.
- *Regulatory perimeter and oversight*. Shared sequencers, data-availability layers and cross-chain messaging services increasingly perform functions similar to those of traditional market infrastructures. As these components grow in scale, they may warrant governance arrangements, resilience standards and supervisory attention comparable to those applied to FMIs.
- *Competition versus standardisation*. Open and interoperable standards can help reduce fragmentation while preserving innovation and competition among platforms. At the same time, cross-border coordination may be needed to mitigate operational risks and regulatory arbitrage, as activities span multiple jurisdictions and infrastructures.

Ultimately, the case for decentralisation is strongest in environments where trust is limited and reliance on central intermediaries is costly or impractical. Still, sustaining robust consensus equilibria at scale requires careful calibration of incentives, transparent governance and effective operational controls. Where permissionless systems take on more mainstream or infrastructure-like roles, the trade-offs inherent in their design should be made explicit and managed in ways that prioritise resilience and accountability, with particular scrutiny of shared components that could become systemically important.

References

Auer, R, C Monnet and H S Shin (2025): "Distributed ledgers and the governance of money", *Journal of Financial Economics*, vol 167, 104026.

Bains, P (2025): "Blockchain consensus mechanisms: a primer for supervisors", *IMF Working Papers*, no 186.

Bank for International Settlements (BIS) (2022): "The future monetary system", *Annual Economic Report 2022*, Chapter III.

Boissay, F, G Cornelli, S Doerr and J Frost (2022): "Blockchain scalability and the fragmentation of crypto", *BIS Bulletin*, no 56.

Budish, E (2025): "Trust at scale: the economic limits of cryptocurrencies and blockchains", *Quarterly Journal of Economics*, vol 140, no 1.

Buterin, V (2021): "Why sharding is great: demystifying the technical properties", available at https://vitalik.eth.limo/general/2021/04/07/sharding.html.

Saleh, F (2021): "Blockchain without waste: proof-of-stake", *Review of Financial Studies*, vol 34, no 3.

Shin, H S (2026): "Tokenomics and blockchain fragmentation", *BIS Working Papers*, no 1335.