Daniel Eidan daniel.eidan@bisih.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@bisih.org

Online appendix for BIS Bulletin no 126: "Blockchain consensus mechanisms and fragmentation"

The design of permissionless blockchains is shaped by the blockchain trilemma: the trade-offs between decentralisation, security and scalability. These trade-offs have led to the emergence of numerous layer 1 (L1) blockchains that differ along these three dimensions. Table A.1 gives examples of major L1 consensus mechanisms and their degree of decentralisation, security and scalability.

At the same time, layer 2 (L2) solutions and sidechains have been developed to reduce fees, improve transaction speed and increase the scalability of L1s. L2 networks process transactions off-chain or in parallel chains, anchoring settlement to an L1. By contrast, sidechains run in parallel and rely on their own validator sets rather than inheriting the security of an L1 network. Table A.2 summarises key L2 solutions, interoperability mechanisms and sidechains, giving examples, mechanisms, security assumptions and impacts on fragmentation.

Finally, this appendix includes a glossary of key terms used in the Bulletin.

Layer 1 consensus designs and indicative trilemma trade-offs[1] Table A.1

Consensus mechanism	Decentralisation	Security	Scalability	Notes
Proof of work (PoW)	High	High (costly to attack)	Low throughput; ~10-minute blocks	Energy consumption reflects PoW's security requirements. Mining hardware and capital intensity raise barriers to entry, which can affect effective decentralisation and scalability.
Proof of stake (PoS)	Moderate–high (high number of validators but staking concentration risk)	High	Moderate (on base layer); scalability via L2s	Ethereum scales by shifting execution to L2 rollups, which process transactions off-chain and post transaction data and state commitments to Ethereum for settlement and data availability.
Proof of stake (PoS) with proof of history (PoH) and Tower BFT	Moderate (hardware-intensive)	Moderate–high	Very high throughput; low-latency confirmation	Uses PoH to pre-order transactions and Tower BFT for consensus. High hardware requirements narrow the participation of validators, limiting decentralisation.
Snow consensus (Snowball/ Snowman) based on probabilistic sampling	Moderate (varies by subnet)	Moderate–high (fast probabilistic finality)	High throughput; low-latency finality	Repeated subsampled voting underpins efficiency. Flexible subnets enable custom validator sets and governance. Decentralisation and interoperability vary by subnet.
Delegated proof of stake (DPoS) with 27 elected super representatives	Low–moderate	Moderate	High throughput; ~3-second blocks	Election-based governance concentrates validation in 27 super representatives, enhancing scalability but reducing decentralisation.
Proof of staked authority (PoSA) with a small, permissioned validator set	Low–moderate	Moderate–high	High throughput	A small, permissioned validator set with high staking requirements boosts performance but concentrates governance and reduces decentralisation. EVM compatibility eases deployment of Ethereum-based applications.
Unique node list (UNL)-based BFT-style consensus with supermajority agreement	Low (curated validator lists)	High (deterministic finality within the chosen validator set)	High throughput; ~3- to 5-second finality	Operators choose UNLs, but many follow default lists maintained by institutions. This yields deterministic finality and efficiency but reduces decentralisation. No token-based validation incentives.

BFT = Byzantine fault tolerance (consensus methods that keep working even if some validators are faulty or malicious); EVM = Ethereum virtual machine (a computation engine that executes smart contracts); SVM = Solana virtual machine.

[1] The indicative trilemma trade-off levels are approximations derived from relative design assessments and comparison with other networks, not absolute evaluations.

Sources: Avalanche (2020); Binance (2020); Buterin (2021); Chase and MacBrough (2018); Nakamoto (2008); Tron (2018); Yakovenko (2017); authors' elaboration.

Layer 2 solutions, interoperability mechanisms and sidechains Table A.2

Category	Example	Mechanism	Security assumption	Fragmentation impact
Layer 2 ecosystem				
Optimistic rollup	Optimism (OP Stack/Superchain), Arbitrum	Transactions are executed off-chain and posted to Ethereum; fraud proofs[3] allow invalid transactions to be challenged	Inherits Ethereum security; assumes at least one honest participant can challenge invalid transactions	Improves scalability but creates separate execution environments and liquidity pools, fragmenting assets
Zero-knowledge rollup	zkSync Era, Starknet, Linea	Transactions are verified using validity proofs[4] before settlement on Ethereum	Validity proofs verified on Ethereum provide strong security guarantees	Offers high security and faster finality than optimistic rollups (no challenge period) but ecosystems often remain siloed, limiting interoperability
Validiums	StarkEx	Transactions use off-chain data storage with validity proofs	Security depends on external data availability committees	Reduces on-chain data requirements but introduces external trust dependencies, fragmenting security guarantees
State channels	Lightning	Off-chain repeated interactions with periodic settlement on L1	Relies on participants (typically in bilateral channels) to monitor and resolve disputes on L1	Reduces on-chain data requirements but suited only for specific bilateral use cases, limiting broader adoption
Interoperability mechanisms				
Cosmos	Cosmos Inter-Blockchain Communication (IBC)	Light client-based[5] message-passing between chains, enabling cross-chain communication within the Cosmos ecosystem	Chains verify each other's state using on-chain light clients	Reduces fragmentation within the Cosmos ecosystem but does not address interoperability with external chains
Cross-chain messaging	LayerZero, Chainlink CCIP, Wormhole, Hyperlane, Axelar	Enables communication between chains using relayers, oracles or validator networks[6]	Depends on the security and honesty of the messaging network	Enables cross-chain interaction but introduces additional trust dependencies and risks
Native multichain issuance	USDC, USDT	Issuers mint native tokens directly across multiple chains, bypassing bridges	Relies on issuer coordination and treasury management	Improves user experience but deepens fragmentation due to separate liquidity pools and operational burden on issuers
Shared infrastructure layer	Celestia (data availability), EigenLayer (shared security)	Dedicated infrastructure layer that stores transaction data for rollups or provides shared security across multiple chains	Security depends on the data availability or shared security network[7]	Reduces duplication of infrastructure but introduces shared dependencies that could become systemic risks

Bridge	Stargate	Assets are locked on one chain while representations (wrapped assets[8]) are minted on another	Depends on bridge contracts and operators (validators/relayers)	Enables asset transfers but creates wrapped assets and additional security risks, including smart contract vulnerabilities
Independent sidechains				
Sidechain[2]	Polygon (Ethereum), Liquid network (Bitcoin)	Independent blockchain that runs in parallel to a parent chain, connected by mechanisms like two-way pegs[9]	Security depends on its own validator set rather than the base chain	Enables lower-cost transactions but creates parallel ecosystems with independent security assumptions

CCIP = Cross-Chain Interoperability Protocol

[1] Rollups process a large number of transactions on layer 2 and record only the aggregated data on the layer 1, reducing on-chain load while inheriting layer 1 security. [2] Sidechains use their own consensus mechanism for security, operating independently from the parent chain. While they enhance scalability, they do not inherit the parent chain's security and are categorised separately from layer 2 solutions. [3] Fraud proofs allow participants to challenge incorrect transactions by providing evidence. If no challenge is made within a set period, the transaction is assumed valid. [4] Validity proofs use cryptography to verify the correctness of transactions without exposing sensitive information, ensuring strong security. [5] Lightweight nodes store only essential blockchain data, enabling efficient cross-chain message-passing while reducing resource requirements. [6] Relayers, oracles and validator networks are intermediaries that facilitate secure communication, data exchange and cross-chain interaction. [7] Data availability networks ensure that transaction data are accessible to all participants, allowing rollups to function securely without duplicating storage. Shared security networks enable multiple protocols to rely on a common validator or staking base, reducing operational overhead but increasing interdependencies. [8] Wrapped assets are tokenised representations of assets locked on one blockchain and minted on another, enabling cross-chain transfers but introducing additional trust and security risks. [9] Two-way pegs are mechanisms that allow assets to move between a parent chain and a sidechain by locking assets on one chain and minting equivalent representations on the other.

Sources: Ethereum (2026); Chainlink (2023); Cosmos (2026); authors' elaboration.

References

Avalanche (2020): *Scalable and probabilistic leaderless BFT consensus through metastability*, white paper, available online at https://www.avalabs.org/whitepapers.

Binance (2020): *BNB smart chain*, white paper, available online at https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md.

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

Chainlink (2023): "What is blockchain interoperability?", available online at https://chain.link/education-hub/blockchain-interoperability.

Chase, B and E MacBrough (2018): "Analysis of the XRP ledger consensus protocol", available online at https://arxiv.org/pdf/1802.07242.

Cosmos (2026): "IBC documentation", available online at https://docs.cosmos.network/ibc/next/intro, accessed on 1 April 2026.

Ethereum (2026): "Ethereum developer documentation", available online at https://ethereum.org/developers/docs/.

Nakamoto, S (2008): *Bitcoin: a peer-to-peer electronic cash system*, white paper.

Tron (2018): *TRON: advancing decentralized applications on blockchain*, white paper, available online at https://tron.network/static/doc/white_paper_v_2_1.pdf.

Yakovenko, A (2017): *Solana: a new architecture for a high-performance blockchain*, white paper, available online at https://solana.com/solana-whitepaper.pdf.

Glossary

The following are descriptions of key terms as used in this Bulletin. Terms are used differently in different contexts, and the use of this glossary does not entail any internationally agreed definition.

Blockchain: a form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated.

Bridge: a technique used to transfer cryptoassets between ecosystems by, typically, creating a synthetic representation of a blockchain-specific cryptoasset on a different blockchain.

Byzantine fault tolerance (BFT): a class of consensus methods that allow the system to function correctly even if some validators are faulty or malicious. The name is derived from the Byzantine generals problem. Fault tolerance holds only up to a protocol-specific bound (eg up to one third Byzantine faults in many classical BFT systems).

Consensus: in DLT applications, the process by which validators agree on the ordering and validity of transactions and the resulting state of a distributed ledger, with either probabilistic or deterministic finality depending on the protocol.

Cryptoasset: a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology.

Data availability: the property that the raw transaction data needed to reconstruct the state are published and accessible to all. Robust data availability is essential for rollups so anyone can verify correctness.

Data availability committee (DAC): a permissioned group that attests to data availability for systems like validiums. Security depends on the committee's honesty and operational integrity.

Data availability layer: a specialised network that publishes/stores rollup data so anyone can verify it without each rollup running its own data infrastructure.

Delegated proof of stake: a consensus mechanism whereby token holders use stake-weighted voting to delegate their stake to elect a limited, rotating set of validators who propose and validate blocks on their behalf.

Deterministic finality: the point at which a transaction cannot be reverted once confirmed by the validator set.

Distributed ledger technology (DLT): a means of saving information through a distributed ledger, ie a repeated digital copy of data available at multiple locations.

Ethereum Virtual Machine (EVM): the execution environment for Ethereum-compatible smart contracts. EVM compatibility enables applications to deploy across EVM-based chains with minimal changes.

Fraud proof: a proof used in optimistic rollups that demonstrates a batch or transaction is invalid. Within a challenge window, any honest participant can submit a fraud proof to ensure the invalid state is identified and reverted in order to maintain the integrity of the system.

Layer 1: the base blockchain network that validates, processes and finalises transactions directly on-chain and provides settlement and data availability guarantees for higher layers.

Layer 2: solutions built on the layer 1 network, where most transactions occur off-chain and are only sporadically or periodically reported back to the underlying layer 1 network.

Light client: a client that verifies another blockchain's state using compact data (eg block headers and proofs) rather than storing full blocks, enabling efficient cross-chain verification and messaging.

Native multichain issuance: an issuance model where an entity (eg a stablecoin issuer) mints native tokens on multiple chains rather than relying on bridges, improving user experience while fragmenting liquidity across chains.

Optimistic rollup: a layer 2 design that assumes batches are valid by default and relies on fraud proofs during a challenge period to detect and revert an invalid state. It inherits base-layer security given at least one honest challenger.

Permissioned: a governing body decides and authorises participant activities, permitting designated service providers to deploy smart contracts and regulators to view transactions, and permission is required for both users and administrators.

Permissionless: all participants may view, edit and conduct activities on the platform, including deploying smart contracts, and no authorisation is required for any activity for either users or administrators.

Probabilistic finality: the probability of reversal decreases over time as more blocks are added.

Proof of history (PoH): not a standalone consensus mechanism, but a cryptographic time-stamping/ordering technique that provides a verifiable sequence of events; used alongside PoS and BFT consensus (eg in Solana) to help order transactions.

Proof of stake (PoS): a consensus mechanism for validating entries into a distributed database and keeping the database secure based on validators' pledging or "staking" a certain amount of cryptoassets in order to have a chance to be chosen for the creation of a new block. Selection probability typically scales with stake; misbehaviour can be penalised via "slashing"; and security relies on economic incentives and honest-majority assumptions.

Proof of staked authority (PoSA): a consensus mechanism whereby a small, permissioned, governance-approved validator set is selected based on a combination of stake and authority.

Proof of work (PoW): a consensus mechanism for validating entries into a distributed database and keeping the database secure. Potential validators compete with one another to solve cryptographic puzzles by expending energy to find a nonce that meets a network difficulty target; security derives from the cost of redoing work.

Rollup: a scaling solution that increases throughput and reduces transaction fees by bundling multiple transactions off-chain (layer 2). It submits batches of data and/or proofs them as a single batch to the main blockchain (layer 1), inheriting layer 1 security (eg via fraud or validity proofs).

Sequencer: a service (often a specific node set) that orders transactions and produces batches for a rollup. A shared sequencer provides ordering for multiple rollups, improving coordination but concentrating operational risk.

Shared security: an arrangement where multiple chains or rollups rely on a common validator/stake set for security, reducing duplication but increasing interdependencies and correlated risk.

Sidechains: independent blockchains that help to overcome capacity restrictions inherent to traditional blockchains by leveraging a separate and independently run network that is connected to the original one by a two-way peg/bridge; sidechains use their own consensus and do not inherit layer 1 security.

Staking/slashing: an incentive mechanism used in PoS family systems by which participants lock up ("stake") native tokens and are selected to propose/verify blocks; misbehaviour can result in part of the stake being forfeited ("slashing").

State: the complete set of on-chain data at a specific block height. It is the result of applying all valid transactions from genesis up to that block and serves as the input for processing the next block.

State channel: an off-chain mechanism for repeated interactions between parties with only occasional on-chain settlements; it is well suited to bilateral, high-frequency use cases.

State commitment: a cryptographic digest (eg a Merkle/Verkle root) posted to a base chain that summarises the rollup's resulting state after a batch, enabling on-chain verification.

Subnet: in Avalanche, a subset of validators that validate one or more blockchains. Subnet membership and rules can be permissionless or permissioned, so decentralisation and security vary by subnet.

Tokenomics: the economic design, governance and incentive structures that allow tokenised networks to function. This includes issuance schedules, fee mechanisms and validator/user incentives.

Two-way peg: a mechanism that enables assets to move between a parent chain and a sidechain by locking assets on one chain and minting/burning equivalent representations on the other.

Unique node list (UNL): in the XRP Ledger, the curated list of validators a node trusts for consensus. Deterministic finality holds within the chosen UNL; effective decentralisation depends on the diversity of UNLs used by network participants.

Validator: a node that participates in consensus by proposing and/or validating blocks according to protocol rules. In permissionless systems, validator participation is open (subject to costs/rules); in permissioned systems, membership is restricted.

Validity proof: a succinct cryptographic proof (eg zero-knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) or zero-knowledge Scalable Transparent Argument of Knowledge (STARK) that attests that a batch of transactions was executed correctly. Verifying the proof on the base chain allows secure settlement without re-execution.

Validium: a system that uses validity proofs for correctness but keeps data off-chain (eg with a DAC), reducing on-chain load while introducing external trust for data availability.

Wrapped asset: a tokenised representation of an asset locked on one blockchain and minted on another (typically via a bridge). Wrapped assets introduce additional trust and smart contract risks.

Zero-knowledge rollup: a layer 2 design that posts validity proofs to the base layer, enabling fast finality and strong security without a challenge period.