STOKR

Sustainability indicators for crypto-assets

Disclosures pursuant to Article 66(5) MiCA

This report was provided by:

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

2026-09-11

Table of Contents

Preamble

About the Crypto-Asset Service Provider (CASP)

Name of the CASP: STOKR S.A.
Street and number: 9 rue du Laboratoire
City: Luxemburg
Country: Luxembourg
LEI: 984500BA521C5EMR1D63

About this report

This disclosure serves as evidence of compliance with the regulatory requirements of Article 66(5) MiCA. Under this provision, crypto-asset service providers are required to disclose information on the principal adverse impacts on the climate and the environment. In particular, this disclosure complies with "Commission Delegated Regulation (EU) 2025/422 of 17 December 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts". The optional information referred to in Article 6(8), points (a) to (d), of Delegated Regulation (EU) 2025/422 is not included.

This report remains valid until material changes occur in the underlying data, in which case it will be updated promptly.

Overview

This is an overview of the core indicator "energy consumption" and does not constitute the disclosure required under Article 66(5) MiCA. The full disclosure is set out below.

#	Crypto-Asset Name	Crypto-Asset FFG	Energy consumption (kWh per calendar year)
1	Bitcoin	V15WLZJMF	156,787,610,364.18
2	USDC	TJWK5QTRK	457,916.74
3	Bitcoin Liquid	M3NCNSV6B	15,373.80
4	Quantoz USDQ	XL2ZV90NC	118.41

Sustainability indicators

Bitcoin

BTC | V15WLZJMF

Quantitative information

Quantitative sustainability indicators for Bitcoin

Field	Value	Unit
S.1 Name	STOKR S.A.	/
S.2 Relevant legal entity identifier	984500BA521C5EMR1D63	/
S.3 Name of the crypto-asset	Bitcoin	/
S.6 Beginning of the period to which the disclosure relates	2025-09-11	/
S.7 End of the period to which the disclosure relates	2026-09-11	/
S.8 Energy consumption	156787610364.17752	kWh/a
S.10 Renewable energy consumption	34.4781471084	%
S.11 Energy intensity	4.48089	kWh
S.12 Scope 1 DLT GHG emissions – Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emissions – Purchased	64595877.93553	tCO2e
S.14 GHG intensity	1.84611	kgCO2e

Qualitative information

S.4 Consensus Mechanism

Bitcoin is present on the following networks: Bitcoin, Lightning Network.

The Bitcoin blockchain network uses a consensus mechanism called Proof of Work (PoW) to achieve distributed consensus among its nodes. Here's a detailed breakdown of how it works:

Core Concepts:

1. Nodes and Miners:
   - Nodes: Nodes are computers running the Bitcoin software that participate in the network by validating transactions and blocks.
   - Miners: Special nodes, called miners, perform the work of creating new blocks by solving complex cryptographic puzzles.

2. Blockchain: The blockchain is a public ledger that records all Bitcoin transactions in a series of blocks. Each block contains a list of transactions, a reference to the previous block (hash), a timestamp, and a nonce (a random number used once).
3. Hash Functions: Bitcoin uses the SHA-256 cryptographic hash function to secure the data in blocks. A hash function takes input data and produces a fixed-size string of characters, which appears random.

Consensus Process:

1. Transaction Validation: Transactions are broadcast to the network and collected by miners into a block. Each transaction must be validated by nodes to ensure it follows the network's rules, such as correct signatures and sufficient funds.
2. Mining and Block Creation:
   - Nonce and Hash Puzzle: Miners compete to find a nonce that, when combined with the block's data and passed through the SHA-256 hash function, produces a hash that is less than a target value. This target value is adjusted periodically to ensure that blocks are mined approximately every 10 minutes.
   - Proof of Work: The process of finding this nonce is computationally intensive and requires significant energy and resources. Once a miner finds a valid nonce, they broadcast the newly mined block to the network.
3. Block Validation and Addition: Other nodes in the network verify the new block to ensure the hash is correct and that all transactions within the block are valid. If the block is valid, nodes add it to their copy of the blockchain and the process starts again with the next block.
4. Chain Consensus: The longest chain (the chain with the most accumulated proof of work) is considered the valid chain by the network. Nodes always work to extend the longest valid chain. In the case of multiple valid chains (forks), the network will eventually resolve the fork by continuing to mine and extending one chain until it becomes longer.

For the calculation of the corresponding indicators, the additional energy consumption and the transactions of the Lightning Network have also been taken into account, as this reflects the categorization of the Digital Token Identifier Foundation for the respective functionally fungible group (“FFG”) relevant for this reporting. If one would exclude these transactions, the respective estimations regarding the “per transaction” count would be substantially higher.

S.5 Incentive Mechanisms and Applicable Fees

Bitcoin is present on the following networks: Bitcoin, Lightning Network.

The Bitcoin blockchain relies on a Proof-of-Work (PoW) consensus mechanism to ensure the security and integrity of transactions. This mechanism involves economic incentives for miners and a fee structure that supports network sustainability:

Incentive Mechanisms:

1. Block Rewards:
   - Newly Minted Bitcoins: Miners are incentivized by block rewards, which consist of newly created bitcoins awarded to the miner who successfully mines a new block. Initially, the block reward was 50 BTC, but it halves every 210,000 blocks (approx. every four years) in an event known as the "halving."
   - Halving and Scarcity: The halving mechanism ensures that the total supply of Bitcoin is capped at 21 million, creating scarcity and potentially increasing value over time.

2. Transaction Fees:
   - User Fees: Each transaction includes a fee paid by the user to incentivize miners to include their transaction in a block. These fees are crucial, especially as the block reward diminishes over time due to halving.
   - Fee Market: Transaction fees are determined by the market, where users compete to have their transactions processed quickly. Higher fees typically result in faster inclusion in a block, especially during periods of high network congestion.

For the calculation of the corresponding indicators, the additional energy consumption and the transactions of the Lightning Network have also been taken into account, as this reflects the categorization of the Digital Token Identifier Foundation for the respective functionally fungible group ("FFG") relevant for this reporting. If one would exclude these transactions, the respective estimations regarding the "per transaction" count would be substantially higher

S.9 Energy consumption sources and methodologies

The energy consumption of this asset is aggregated across multiple components:

For the calculation of energy consumptions, the so called 'top-down' approach is being used, within which an economic calculation of the miners is assumed. Miners are persons or devices that actively participate in the proof-of-work consensus mechanism. The miners are considered to be the central factor for the energy consumption of the network. Hardware is pre-selected based on the consensus mechanism's hash algorithm: SHA-256. A current profitability threshold is determined on the basis of the revenue and cost structure for mining operations. Only Hardware above the profitability threshold is considered for the network. The energy consumption of the network can be determined by taking into account the distribution for the hardware, the efficiency levels for operating the hardware and on-chain information regarding the miners' revenue opportunities. If significant use of merge mining is known, this is taken into account. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset of question in scope and we update the mappings regulary, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

To determine the energy consumption of a token, the energy consumption of the network(s) lightning_network is calculated first. For the energy consumption of the token, a fraction of the energy consumption of the network is attributed to the token, which is determined based on the activity of the crypto-asset within the network. When calculating the energy consumption, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used - if available - to determine all implementations of the asset in scope. The mappings are updated regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If

no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal energy cost wrt. one more transaction.

Ember (2025); Energy Institute - Statistical Review of World Energy (2024) - with major processing by Our World in Data. "Share of electricity generated by renewables - Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from https://ourworldindata.org/grapher/share-electricity-renewables.

S.16 Key GHG sources and methodologies

To determine the GHG Emissions, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal emission wrt. one more transaction.

Ember (2025); Energy Institute - Statistical Review of World Energy (2024) - with major processing by Our World in Data. "Carbon intensity of electricity generation - Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from https://ourworldindata.org/grapher/carbon-intensity-electricity Licenced under CC BY 4.0.

USDC

USDC | TJWK5QTRK

Quantitative information

Quantitative sustainability indicators for USDC

Field	Value	Unit
S.1 Name	STOKR S.A.	/
S.2 Relevant legal entity identifier	984500BA521C5EMR1D63	/
S.3 Name of the crypto-asset	USDC	/
S.6 Beginning of the period to which the disclosure relates	2025-09-11	/
S.7 End of the period to which the disclosure relates	2026-09-11	/
S.8 Energy consumption	457916.73520	kWh/a

Qualitative information

S.4 Consensus Mechanism

USDC is present on the following networks: Algorand, Aptos Coin, Arbitrum, Avalanche, Base, Celo, Ethereum, Flow, Hedera Hbar, Hyperliquid, Injective, Linea, Near Protocol, Optimism, Plume, Polygon, Ripple, Sei, Solana, Sonic, Starknet, Statemint, Stellar, Sui, Tron, Xdc Network, Zksync.

The Algorand blockchain utilizes a consensus mechanism termed Pure Proof-of-Stake (PPoS). Consensus, in this context, describes the method by which blocks are selected and appended to the blockchain. Algorand employs a verifiable random function (VRF) to select leaders who propose blocks for each round.

Upon block proposal, a pseudorandomly selected committee of voters is chosen to evaluate the proposal. If a supermajority of these votes are from honest participants, the block is certified. What makes this algorithm a Pure Proof of Stake is that users are chosen for committees based on the number of algos in their accounts. This system leverages random committee selection to maintain high performance and inclusivity within the network.

The consensus process involves three stages:

1. Propose: A leader proposes a new block.
2. Soft Vote: A committee of voters assesses the proposed block.
3. Certify Vote: Another committee certifies the block if it meets the required honesty threshold.

Aptos utilizes a Proof-of-Stake approach combined with a BFT consensus protocol to ensure high throughput, low latency, and secure transaction processing.

Core Components:

- Parallel Execution: Transactions are processed concurrently using Block-STM, a parallel execution engine, enabling high performance and scalability.
- Leader-Based BFT: A leader is selected among validators to propose blocks, while others validate and finalize transactions.
- Dynamic Validator Rotation: Validators are rotated regularly, enhancing decentralization and preventing collusion.
- Instant Finality: Transactions achieve finality once validated, ensuring that they are irreversible.

Arbitrum is an optimistic rollup that processes transactions on a Layer 2 network and relies on Ethereum for data availability and settlement. A sequencer orders incoming transactions, executes them and publishes compressed transaction batches to Ethereum. Arbitrum nodes can independently reconstruct and verify the resulting Layer 2 state using the transaction data published on the parent chain. Validators submit assertions representing the state of the network. Under the BoLD dispute protocol, conflicting or incorrect assertions may be challenged and resolved through an interactive fraud-proof process on Ethereum. Once an assertion has been confirmed and the applicable challenge process has been completed, the corresponding Layer 2 state is accepted for settlement purposes.

The Avalanche C-Chain uses the Snowman++ consensus mechanism, which is Avalanche's consensus model for linear blockchains and is implemented through the ProposerVM wrapper. Under this model, validators repeatedly query a small random subset of other validators and converge on a preferred block once the required confidence thresholds are met. Only Primary Network validators are entitled to validate the C-Chain. To participate as a validator on Avalanche mainnet, a node must stake a minimum number of token. Token holders may also participate indirectly by delegating an existing validator. Validator identity and admission to staking require the relevant staking credentials, including BLS proofs of possession under the current staking framework. For block production, Snowman++ uses stake-weighted proposer windows. Through the ProposerVM, block-building opportunities are assigned to proposers in 5-second windows, after which block production may fall back more broadly to validators if necessary. This mechanism is intended to regulate block production while preserving network liveness. Consensus voting itself remains based on repeated sub-sampled polling rather than fixed validator committees. Avalanche documentation describes the finality model as sub-second and treated by the protocol as final and irreversible once accepted, while noting that safety is probabilistic in the formal sense because the probability of conflicting acceptance can be reduced to an arbitrarily low level through the protocol parameters. The protocol does not rely on slashing of staked principal. Instead, validator reward eligibility depends on compliance with protocol conditions, including uptime requirements.

Base does not operate its own consensus mechanism or decentralised validator set comparable to a Layer-1 blockchain. As an optimistic rollup Layer-2 network, Base relies on Ethereum's Proof-of-Stake consensus for the finality and settlement of data and state commitments posted to Ethereum Layer 1. Transaction ordering on Base is performed by a sequencer, currently operated by Coinbase. This sequencing function provides transaction ordering and execution on the Layer-2 network but does not constitute a decentralised consensus mechanism. The validity of Layer-2 state transitions is supported by an optimistic fault-proof mechanism, under which incorrect state commitments may be challenged during the applicable dispute period. Accordingly, Base's security model depends on Ethereum Layer 1 for settlement and finality, while Layer-2 transaction ordering remains dependent on the sequencer.

Celo uses a Proof of Stake (PoS) consensus model, which supports a decentralized, community-driven approach to governance and network security.

Core Components of Celo's Consensus:

1. Proof of Stake (PoS):
   Validator Role: Validators are responsible for creating new blocks, validating transactions, and maintaining the security and integrity of the network. Validators are selected based on the amount of CELO tokens they hold and stake, incentivizing honest participation and network reliability.
2. Decentralized Governance:
   Community Voting: Governance on Celo is decentralized, allowing CELO token holders to vote on proposals and changes to the network. This community-driven approach ensures that token holders have a say in the network's development and strategic direction.

Ethereum uses a Proof-of-Stake (PoS) consensus mechanism introduced with The Merge on 2022-09-15, which replaced the previous Proof-of-Work consensus model. The PoS mechanism is implemented through Gasper, combining Casper-FFG for finality with the LMD-GHOST fork-choice rule for chain selection. Validators participate in consensus by staking ETH through the Beacon Chain. Validators are pseudo-randomly selected to propose new blocks, while other validators attest to the validity of proposed blocks. The network operates using 12-second slots grouped into epochs of 32 slots. Under normal network conditions, finality is typically achieved after two epochs, approximately 12.8 minutes, through Casper-FFG. The LMD-GHOST fork-choice rule determines the canonical chain based on the accumulated weight of validator attestations. Validators that engage in certain malicious behaviour, such as equivocation or contradictory attestations, may be subject to slashing penalties, while offline validators may incur inactivity penalties. Subsequent network upgrades, including Dencun (2024-03-13), Pectra (2025-05-07) and Fusaka (2025-12-03), introduced protocol changes affecting Ethereum's consensus mechanism and Layer 2 functionality.

Flow employs a Proof of Stake (PoS) model with a multi-role node architecture and the HotStuff Byzantine Fault Tolerant (BFT) protocol to achieve high throughput, scalability, and fast finality.

Core Components of Flow's Consensus:

1. Proof of Stake with Multi-Role Architecture:
   Specialized Node Roles: Flow's PoS model features a multi-node architecture where node roles are divided among different types of specialized nodes, each responsible for specific tasks. This separation enhances scalability by allowing nodes to focus on particular operations, leading to efficient transaction processing and high throughput.
2. HotStuff Consensus Algorithm:
   - Optimized for High Throughput and Fast Finality: Flow utilizes an optimized version of the HotStuff consensus protocol, which is designed to support high-speed, low-latency transactions essential for Flow's performance-oriented blockchain.
   - BFT Compliance: HotStuff is a BFT protocol, allowing it to tolerate up to one-third of nodes acting maliciously without compromising the network's security. This resilience ensures the network remains secure and functional, even with potential faults or dishonest nodes.
3. Leader-Based Block Proposal:
   - Leader and Replica Nodes: HotStuff operates with a leader-based approach where a designated leader node proposes new blocks, and other nodes (replicas) validate these blocks. This method simplifies the consensus process, reducing complexity and improving efficiency.
   - Leader Rotation Mechanism: To prevent centralization and enhance fault tolerance, HotStuff incorporates a leader rotation system, replacing the leader if it becomes unresponsive or acts maliciously. This rotation ensures continuous network reliability and minimizes downtime.

Hedera Hashgraph operates on a unique Hashgraph consensus algorithm, a directed acyclic graph (DAG) system that diverges from traditional blockchain technology. It uses Asynchronous Byzantine Fault Tolerance (aBFT) to secure the network.

Core Components:

1. Hashgraph Consensus and aBFT:
   Hedera Hashgraph's consensus mechanism achieves aBFT, which allows the network to tolerate malicious nodes without compromising security, ensuring high levels of fault tolerance and stability.
2. Gossip about Gossip Protocol:
   The network employs a "Gossip about Gossip" protocol, where nodes share transaction information along with details of previous gossip events. This process allows each node to rapidly learn the entire network state, enhancing communication efficiency and minimizing latency.
3. Virtual Voting:
   Hedera does not rely on traditional miners or stakers. Instead, it uses virtual voting, where nodes reach consensus by analyzing the gossip history and simulating votes based on the order and frequency of transactions received. Virtual voting eliminates the need for actual voting messages, reducing network congestion and speeding up consensus.
4. Deterministic Finality:
   Once consensus is reached, transactions achieve deterministic finality instantly, making them irreversible and confirmed within seconds. This attribute is ideal for applications needing quick and irreversible transaction confirmations.
5. Staking for Network Security:
   Hedera incorporates staking to bolster network security. HBAR holders can stake their tokens to support validator nodes, contributing to the network's resilience and encouraging long-term engagement in consensus operations.

Hyperliquid is a decentralized perpetual exchange (DEX) built on its proprietary Layer 1 blockchain, Hyperliquid L1. At the core of its architecture is the HyperBFT consensus mechanism, inspired by the Hotstuff protocol, designed to meet the demands of high-frequency trading while maintaining security and consistency across the ecosystem.

Injective operates on a Tendermint-based Proof of Stake (PoS) consensus model, ensuring high throughput and immediate transaction finality.

Core Components:

- Tendermint-based Proof of Stake (PoS):
  Ensures instant transaction finality and supports efficient block production for high-speed transactions.
- Validator Selection:
  Validators are chosen based on the amount of INJ tokens staked, considering both self-staked and delegated tokens, to maintain a decentralized network.
- Delegation:
  INJ holders can delegate their tokens to validators, earning a share of staking rewards while participating in network governance.
- Instant Finality:
  The Tendermint consensus mechanism provides immediate finality, ensuring transactions cannot be reversed once validated.

The Linea Network uses a Zero-Knowledge Rollup (ZK-Rollup) architecture with a zkEVM for Ethereum compatibility, and its consensus is derived from Ethereum's own proof-of-stake security. While the Network has components like a sequencer for ordering transactions and a coordinator for network management, its consensus mechanism is fundamentally linked to the proof and verification process of zero-knowledge proofs and the security of the Ethereum mainnet. Instead of a typical decentralized consensus on a separate blockchain, the Network inherits its security and state finality from Ethereum.

The NEAR Protocol uses a unique consensus mechanism combining Proof of Stake (PoS) and a novel approach called Doomslug, which enables high efficiency, fast transaction processing, and secure finality in its operations.

Core Concepts:

1. Doomslug and Proof of Stake:
   - NEAR's consensus mechanism primarily revolves around PoS, where validators stake NEAR tokens to participate in securing the network. However, NEAR's implementation is enhanced with the Doomslug protocol.
   - Doomslug allows the network to achieve fast block finality by requiring blocks to be confirmed in two stages. Validators propose blocks in the first step, and finalization occurs when two-thirds of validators approve the block, ensuring rapid transaction confirmation.
2. Sharding with Nightshade:
   - NEAR uses a dynamic sharding technique called Nightshade. This method splits the network into multiple shards, enabling parallel processing of transactions across the network, thus significantly increasing throughput. Each shard processes a portion of transactions, and the outcomes are merged into a single "snapshot" block.
   - This sharding approach ensures scalability, allowing the network to grow and handle increasing demand efficiently.

Consensus Process:

1. Validator Selection:
   - Validators are selected to propose and validate blocks based on the amount of NEAR tokens staked. This selection process is designed to ensure that only validators with significant stakes and community trust participate in securing the network.
2. Transaction Finality:
   - NEAR achieves transaction finality through its PoS-based system, where validators vote on blocks. Once two-thirds of validators approve a block, it reaches finality under Doomslug, meaning that no forks can alter the confirmed state.
3. Epochs and Rotation:
   - Validators are rotated in epochs to ensure fairness and decentralization. Epochs are intervals in which validators are reshuffled, and new block proposers are selected, ensuring a balance between performance and decentralization.

Since Optimism is based on Ethereum, it ultimately inherits its security via the Ethereum blockchain and the proof-of-stake consensus. Within the rollup system, Optimism relies on a “fault proof” procedure. By default, transactions are assumed to be correct (“optimistic”). Only in the event of suspected faults is a fault proof initiated, in which incorrect transactions can be challenged by challengers. This model allows for high efficiency while ensuring correctness.

Plume is described as relying on an architecture aligned with optimistic rollup technology within the Arbitrum Orbit framework. Under this design, transaction ordering is typically performed by a sequencer, while settlement and finality are achieved via anchoring to Ethereum. Economic

incentives and protocol rules are generally designed to encourage timely submission of fraud proofs (where applicable) within predefined challenge windows. The precise security guarantees and finality characteristics depend on the rollup configuration, the sequencer setup, and Ethereum's underlying security assumptions.

Polygon PoS is an EVM-compatible sidechain that operates with a Proof-of-Stake consensus mechanism and periodically submits checkpoints to the Ethereum mainnet. The network maintains its own validator set and processes transactions independently from Ethereum, while using Ethereum smart contracts for staking-related functions and checkpoint verification. Polygon PoS therefore uses Ethereum as a staking and checkpointing layer, but does not rely on Ethereum for full transaction execution or transaction data availability. The Polygon-side architecture consists of two primary node layers. The Bor layer is responsible for transaction execution and block production. The Heimdall layer is responsible for validator coordination, staking-related monitoring, consensus, and checkpoint finalisation. Heimdall is based on Cosmos SDK and CometBFT and aggregates blocks produced by Bor into periodic Merkle-root checkpoints that are submitted to smart contracts on the Ethereum mainnet. Validators participate in the network by staking POL tokens. Token holders may delegate POL tokens to validators, contributing to the validator's effective stake and participating indirectly in network validation. Following the Rio upgrade, Polygon PoS uses a Validator-Elected Block Producer model. Under this model, validators elect the block producer or block producers for a span, rather than relying on the previous stake-weighted selection model for multiple block producers over shorter intervals. Block production and transaction execution are performed on the Bor layer, while Heimdall validators coordinate consensus and checkpoint finalisation. At regular intervals, Heimdall validators aggregate blocks into a Merkle root and submit the resulting checkpoint to Ethereum smart contracts. These checkpoints provide an additional verification layer and support cross-chain verification, including in the context of asset transfers between Polygon PoS and Ethereum. This design enables higher transaction throughput and lower transaction costs than the Ethereum mainnet, while maintaining a technical connection to Ethereum through staking contracts and periodic checkpointing. Polygon PoS should therefore be understood as an independent sidechain or commit-chain architecture, rather than a rollup that inherits full execution and data availability security from Ethereum.

The Ripple blockchain, specifically the XRP Ledger (XRPL), uses a consensus mechanism known as the Ripple Protocol Consensus Algorithm (RPCA). It differs from Proof of Work (PoW) and Proof of Stake (PoS) as it doesn't rely on mining or staking but instead leverages trusted validators in a Federated Byzantine Agreement (FBA) model.

Core Concepts:

1. Validators and Unique Node Lists (UNL): Validators are trusted nodes in the network that validate transactions and propose new ledger updates. Each node maintains a list of trusted validators known as its Unique Node List (UNL). Consensus is achieved when 80% of the validators in a node's UNL agree on the validity of a transaction or block. This ensures high levels of security and decentralization.
2. Transaction Ordering and Validation: Transactions are broadcast to validators, and once 80% of the validators agree, the transaction is considered confirmed. Each ledger in the XRPL contains transaction data, and validators ensure the validity and proper ordering of these transactions.

Consensus Process:

1. Proposal Phase: Validators propose new transactions to be added to the ledger.
2. Validation Phase: Validators vote on proposed transactions by comparing them to their UNL. Consensus is achieved when 80% of validators agree.

3. Finalization: Once consensus is reached, the transactions are written into the new ledger, making them irreversible and final.

Sei leverages its Twin-Turbo consensus mechanism, integrating advanced transaction processing techniques with the reliability of Tendermint Core, to achieve high performance and security.

Core Components:

- Twin-Turbo Consensus:
  - Optimistic Block Processing: Validators process transactions optimistically, assuming their validity, reducing latency and increasing throughput.
  - Intelligent Block Propagation: Compressed block proposals containing transaction hashes enable validators to reconstruct blocks locally, expediting consensus.
  - Single Slot Finality: Ensures immediate block finality upon addition, eliminating the need for confirmations and minimizing the risk of chain reorganizations.
- Tendermint Core Integration:
  Incorporates Byzantine Fault Tolerance (BFT) to maintain security and resilience, safeguarding the network against malicious actors.

Solana uses a unique combination of Proof of History (PoH) and Proof of Stake (PoS) to achieve high throughput, low latency, and robust security.

Core Concepts:

1. Proof of History (PoH):
   - Time-Stamped Transactions: PoH is a cryptographic technique that timestamps transactions, creating a historical record that proves that an event has occurred at a specific moment in time.
   - Verifiable Delay Function: PoH uses a Verifiable Delay Function (VDF) to generate a unique hash that includes the transaction and the time it was processed. This sequence of hashes provides a verifiable order of events, enabling the network to efficiently agree on the sequence of transactions.
2. Proof of Stake (PoS):
   - Validator Selection: Validators are chosen to produce new blocks based on the number of SOL tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.
   - Delegation: Token holders can delegate their SOL tokens to validators, earning rewards proportional to their stake while enhancing the network's security.

Consensus Process:

1. Transaction Validation:
   Transactions are broadcast to the network and collected by validators. Each transaction is validated to ensure it meets the network’s criteria, such as having correct signatures and sufficient funds.
2. PoH Sequence Generation:
   A validator generates a sequence of hashes using PoH, each containing a timestamp and the previous hash. This process creates a historical record of transactions, establishing a cryptographic clock for the network.
3. Block Production:
   The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order.

4. Consensus and Finalization:
   Other validators verify the block produced by the leader validator. They check the correctness of the PoH sequence and validate the transactions within the block. Once the block is verified, it is added to the blockchain. Validators sign off on the block, and it is considered finalized.

Security and Economic Incentives:

1. Incentives for Validators:
   - Block Rewards: Validators earn rewards for producing and validating blocks. These rewards are distributed in SOL tokens and are proportional to the validator's stake and performance.
   - Transaction Fees: Validators also earn transaction fees from the transactions included in the blocks they produce. These fees provide an additional incentive for validators to process transactions efficiently.
2. Security:
   - Staking: Validators must stake SOL tokens to participate in the consensus process. This staking acts as collateral, incentivizing validators to act honestly. If a validator behaves maliciously or fails to perform, they risk losing their staked tokens.
   - Delegated Staking: Token holders can delegate their SOL tokens to validators, enhancing network security and decentralization. Delegators share in the rewards and are incentivized to choose reliable validators.
3. Economic Penalties:
   Slashing: Validators can be penalized for malicious behavior, such as double-signing or producing invalid blocks. This penalty, known as slashing, results in the loss of a portion of the staked tokens, discouraging dishonest actions.

Sonic utilizes a Proof-of-Stake (PoS) consensus mechanism integrated with a Directed Acyclic Graph (DAG) architecture to enhance scalability and efficiency. Validators are required to stake the network's native $S tokens, with a minimum of 500,000 $S tokens needed to operate a validator node. This substantial staking requirement ensures that validators have a significant investment in the network's integrity.

Starknet employs zero-knowledge rollups (ZK-Rollups) for transaction aggregation and scalability, ensuring efficiency and security through succinct proof submissions to Ethereum.

Core Components:

- Zero-Knowledge Rollups (ZK-Rollups):
  Aggregates multiple off-chain transactions into a single proof, which is submitted to Ethereum's mainnet, reducing computational load and gas costs.
- Sequencer and Prover Roles:
  - Sequencers: Order and batch transactions for efficient processing.
  - Provers: Generate validity proofs ensuring the correctness of processed batches.
- Instant Finality:
  Transactions are final once a proof is verified and accepted on Ethereum, minimizing the risk of chain reorganizations and enhancing reliability.

Statemint is a common-good parachain on the Polkadot and Kusama networks, designed to handle asset management and issuance efficiently while leveraging Polkadot's shared security model.

Core Components:

- Relay Chain Integration: Statemint inherits its consensus mechanism from the Polkadot Relay Chain, which operates on a Nominated Proof of Stake (NPoS) model. This model ensures robust security and decentralization by relying on validators and nominators.
- Shared Security: As a parachain, Statemint utilizes the Polkadot Relay Chain's validators for block validation, ensuring high security and interoperability without requiring independent validators.
- Collator Nodes: Statemint employs collator nodes to aggregate transactions into blocks and submit them to the Relay Chain validators for finalization. Collators do not participate in consensus directly but play a key role in transaction processing.
- Immediate Finality: The underlying Polkadot consensus mechanism ensures instant finality using the GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) protocol, which provides secure and efficient transaction confirmation.

Consensus is reached through the Stellar Consensus Protocol (SCP), which is based on federated Byzantine agreement. This mechanism allows fast finality without mining or staking, but it depends on validators choosing other validators which they trust to reach agreement, called a quorum set. As a result, validator diversity and governance choices play a critical role in security, and concentration of influence among large operators may increase systemic risks.

The Sui blockchain utilizes a Byzantine Fault Tolerant (BFT) consensus mechanism optimized for high throughput and low latency.

Core Components:

1. Mysten Consensus Protocol:
   - The Sui consensus is based on Mysten Labs' Byzantine Fault Tolerance (BFT) protocol, which builds on principles of Practical Byzantine Fault Tolerance (pBFT) but introduces key optimizations for performance.
   - Leaderless Design: Unlike traditional BFT models, Sui does not rely on a single leader to propose blocks. Validators can propose blocks simultaneously, increasing efficiency and reducing the risks associated with leader failure or attacks.
   - Parallel Processing: Transactions can be processed in parallel, maximizing network throughput by utilizing multiple cores and threads. This allows for faster confirmation of transactions and high scalability.
2. Transaction Validation:
   Validators are responsible for receiving transaction requests from clients and processing them. Each transaction includes digital signatures and must meet the network's rules to be considered valid. Validators can propose transactions simultaneously, unlike many other networks that require a sequential, leader-driven process.
3. Optimistic Execution:
   Optimistic Consensus: Sui allows validators to process certain non-contentious, independent transactions without waiting for full consensus. This is known as optimistic execution and helps reduce transaction latency for many use cases, allowing for fast finality in most cases.
4. Finality and Latency:
   The system only requires three rounds of communication between validators to finalize a transaction. This results in low-latency consensus and rapid transaction confirmation times, achieving scalability while maintaining security.
5. Fault Tolerance:
   The system can tolerate up to one-third of validators being faulty or malicious without compromising the integrity of the consensus process.

The Tron blockchain operates on a Delegated Proof of Stake (DPoS) consensus mechanism, designed to improve scalability, transaction speed, and energy efficiency.

Core Components:

1. Delegated Proof of Stake (DPoS): Tron uses DPoS, where token holders vote for a group of delegates known as Super Representatives (SRs)who are responsible for validating transactions and producing new blocks on the network. Token holders can vote for SRs based on their stake in the Tron network, and the top 27 SRs (or more, depending on the protocol version) are selected to participate in the block production process. SRs take turns producing blocks, which are added to the blockchain. This is done on a rotational basis to ensure decentralization and prevent control by a small group of validators.
2. Block Production: The Super Representatives generate new blocks and confirm transactions. The Tron blockchain achieves block finality quickly, with block production occurring every 3 seconds, making it highly efficient and capable of processing thousands of transactions per second.
3. Voting and Governance: Tron's DPoS system also allows token holders to vote on important network decisions, such as protocol upgrades and changes to the system's parameters. Voting power is proportional to the amount of TRX (Tron's native token) that a user holds and chooses to stake. This provides a governance system where the community can actively participate in decision-making.
4. Super Representatives: The Super Representatives play a crucial role in maintaining the security and stability of the Tron blockchain. They are responsible for validating transactions, proposing new blocks, and ensuring the overall functionality of the network. Super Representatives are incentivized with block rewards (newly minted TRX tokens) and transaction feesfor their work.

XinFin Network operates on a modified Delegated Proof of Stake (XDPoS) model, XDPoS 2.0, which ensures scalability, security, and efficiency suitable for enterprise applications.

Core Components:

1. XDPoS 2.0 (Delegated Proof of Stake):
   Masternode System: Validators, known as masternodes, are required to stake XDC tokens to participate in transaction validation and block production. Validators are selected based on both stake size and community votes, ensuring only reliable nodes secure the network.
2. Double Validation Feature:
   - Enhanced Security: Each transaction is validated by two independent validators before it's finalized, reducing the risk of double-spending or malicious behavior and increasing network reliability.
   - Randomized Validator Rotation: Validators are selected in a rotating and randomized manner, preventing any single validator from consistently producing blocks, which enhances decentralization and security.

zkSync operates as a Layer 2 scaling solution for Ethereum, leveraging zero-knowledge rollups (ZK-Rollups) to enable fast, cost-effective, and secure transactions. This consensus mechanism allows zkSync to offload transaction computation from Ethereum's Layer 1, ensuring scalability while maintaining Ethereum's base-layer security.

Core Components:

- Zero-Knowledge Rollups (ZK-Rollups):
  zkSync aggregates multiple transactions off-chain and processes them in batches. A cryptographic proof, called a validity proof, is generated for each batch and submitted to the Ethereum

mainnet. This ensures that all transactions are valid and compliant with Ethereum's rules without processing them individually on Layer 1.

- Validity Proofs:
  zkSync uses zk-SNARKs (Succinct Non-Interactive Arguments of Knowledge) for its validity proofs. These proofs provide mathematical guarantees that transactions within a batch are valid, eliminating the need for Ethereum nodes to re-execute off-chain transactions.
- Sequencers:
  Transactions on zkSync are ordered and processed by sequencers, which bundle transactions into batches. Sequencers maintain network efficiency and provide fast confirmations.
- Fraud Resistance:
  Unlike Optimistic Rollups, zkSync relies on validity proofs rather than fraud proofs, meaning that transactions are final and secure as soon as the validity proof is accepted by Ethereum.
- Data Availability:
  All transaction data is stored on-chain, ensuring that the network remains decentralized and users can reconstruct the state of zkSync at any time.

S.5 Incentive Mechanisms and Applicable Fees

USDC is present on the following networks: Algorand, Aptos Coin, Arbitrum, Avalanche, Base, Celo, Ethereum, Flow, Hedera Hbar, Hyperliquid, Injective, Linea, Near Protocol, Optimism, Plume, Polygon, Ripple, Sei, Solana, Sonic, Starknet, Statemint, Stellar, Sui, Tron, Xdc Network, Zksync.

Algorand's consensus mechanism, Pure Proof-of-Stake (PPoS), relies on the participation of token holders (stakers) to ensure the network's security and integrity:

1. Participation Rewards:
   - Staking Rewards: Users who participate in the consensus protocol by staking their ALGO tokens earn rewards. These rewards are distributed periodically and are proportional to the amount of ALGO staked. This incentivizes users to hold and stake their tokens, contributing to network security and stability.
   - Node Participation Rewards: Validators, also known as participation nodes, are responsible for proposing and voting on blocks. These nodes receive additional rewards for their active role in maintaining the network.
2. Transaction Fees:
   - Flat Fee Model: Algorand employs a flat fee model for transactions, which ensures predictability and simplicity. The standard transaction fee on Algorand is very low (around 0.001 ALGO per transaction). These fees are paid by users to have their transactions processed and included in a block.
   - Fee Redistribution: Collected transaction fees are redistributed to participants in the network. This includes stakers and validators, further incentivizing their participation and ensuring continuous network operation.
3. Economic Security:
   Token Locking: To participate in the consensus mechanism, users must lock up their ALGO tokens. This economic stake acts as a security deposit that can be slashed (forfeited) if the participant acts maliciously. The potential loss of staked tokens discourages dishonest behavior and helps maintain network integrity.

Fees on the Algorand Blockchain

1. Transaction Fees:
   Algorand uses a flat transaction fee model. The current standard fee is 0.001 ALGO per transaction. This fee is minimal compared to other blockchain networks, ensuring affordability and accessibility.
2. Smart Contract Execution Fees:
   Fees for executing smart contracts on Algorand are also designed to be low. These fees are based on the computational resources required to execute the contract, ensuring that users are only charged for the actual resources they consume.
3. Asset Creation Fees:
   Creating new assets (tokens) on the Algorand blockchain involves a small fee. This fee is necessary to prevent spam and ensure that only genuine assets are created and maintained on the network.

Incentive Mechanism:

- Validator Rewards: Validators earn rewards in APT tokens for validating transactions and producing blocks. Rewards are distributed proportionally based on the stake of validators and their delegators.
- Delegator Participation: APT token holders can delegate their tokens to validators, earning a share of the staking rewards without running their own nodes.
- Slashing Mechanism: Validators face penalties, such as losing staked tokens, for malicious actions or prolonged inactivity, ensuring accountability and network security.

Applicable Fees:

- Transaction Fees: Users pay transaction fees in APT tokens for sending transactions and interacting with smart contracts.
- Dynamic Fee Adjustment: Fees are dynamically adjusted based on network activity and resource usage, ensuring cost efficiency and preventing congestion.
- Fee Distribution: Transaction fees are distributed among validators and delegators, providing an additional incentive for network participation.

Transactions on Arbitrum are subject to fees paid in ETH. The total fee generally consists of a Layer 2 execution component, which covers the computational resources required to process the transaction, and a parent-chain data component, which reflects the cost of publishing compressed transaction data to Ethereum. The amount payable therefore depends on the computational complexity of the transaction, the volume and compressibility of its data and the prevailing cost of data publication on Ethereum. Participants that submit or challenge state assertions under the dispute protocol must provide economic bonds. These bonds are intended to discourage incorrect assertions and compensate successful participants in the dispute process. Withdrawals through the canonical bridge become executable after the relevant Layer 2 state has been confirmed and the applicable challenge period has elapsed.

The Avalanche C-Chain is secured economically through the native AVAX token. Validator incentives are based primarily on staking rewards, not on redistribution of C-Chain transaction fees. A fixed amount of 360 million AVAX was minted at genesis, while additional AVAX is minted over time as validator rewards, subject to Avalanche's capped token supply framework. Validator rewards are paid at the end of the staking period and are determined by factors such as the validator's stake and compliance with staking conditions. Unlike some proof-of-stake systems, the Avalanche Primary Network does not use slashing of bonded principal as an ordinary penalty mechanism. Instead, the main protocol-level economic consequence for underperformance is the loss of reward eligibility.

Where a validator fails to satisfy the applicable uptime requirement during its staking term, that validator does not receive the corresponding staking reward. Transaction fees apply on the C-Chain for transfers and smart-contract execution. The fee model follows EIP-1559 logic, meaning that transactions are priced through a dynamic base fee mechanism. In contrast to Ethereum's validator tip model, C-Chain transaction fees are burned rather than distributed to validators. This means that C-Chain fees function as a supply-reduction mechanism and are intended in part to offset inflation arising from the minting of validator rewards. In addition to ordinary transaction and smart-contract execution fees, Avalanche documentation also recognises protocol fees in connection with other network operations on other chains of the Primary Network, such as certain import or export operations and staking-related actions. However, for the C-Chain itself, the core applicable fee category is the gas fee for transaction inclusion and contract execution, and those fees are handled through the protocol burn mechanism rather than paid to validators or a treasury.

Base does not have a native protocol token and does not operate a staking, validator reward or token issuance mechanism. Transaction fees on Base are paid in ETH. The economic incentives within the network are primarily related to transaction processing and network security. Transactions are executed on Base and periodically submitted to Ethereum Layer 1 in batches. As the cost of a Layer-1 submission is shared among multiple Layer-2 transactions, the average transaction cost per transaction may be lower than executing the same transactions directly on Ethereum Layer 1. The integrity of withdrawals from Base is supported by a fault-proof mechanism. Withdrawals are subject to a dispute period during which participants may challenge incorrect state commitments. The dispute process incorporates economic incentives intended to encourage honest behaviour and discourage invalid claims.

Celo's incentive model rewards validators and prioritizes accessibility with minimal transaction fees, especially for cross-border payments, supporting a flexible and user-friendly ecosystem.

Incentive Mechanisms:

1. Validator Rewards:
   Transaction Fees and Newly Minted Tokens: Validators earn rewards from transaction fees as well as newly minted CELO tokens. This dual-source reward system provides a continuous financial incentive for validators to act honestly and secure the network.
2. Transaction Flexibility and Gas Price:
   - Gas Limit and Price Control: Each transaction specifies a maximum gas limit, ensuring that users are not excessively charged if a transaction fails. Users can also set a gas price to prioritize transactions, allowing faster processing for higher fees.
   - Payment Flexibility with Multiple Currencies: Unlike many blockchains, Celo allows transaction fees to be paid in various ERC-20 tokens, providing flexibility for users. This approach improves accessibility, especially for individuals with limited access to traditional banking.
3. Minimal Fee Structure for Accessibility:
   - Designed for Low-Cost Transactions: Celo's fee structure is intentionally minimal, particularly for cross-border payments, making it ideal for users who may not have traditional banking options. This focus on accessibility aligns with Celo's mission to bring blockchain technology to underserved communities.

Applicable Fees:

Transaction Fees: Fees are calculated based on gas usage, with a maximum gas limit set per transaction. This limit protects users from excessive costs, while the option to pay in multiple currencies enhances flexibility.

Ethereum's Proof-of-Stake (PoS) mechanism secures the network through validator incentives and protocol-defined penalties. Validators are required to stake ETH in order to participate in block proposal and attestation activities. A minimum of 32 ETH is required to activate a validator. Following the Pectra upgrade on 2025-05-07, EIP-7251 increased the maximum effective balance per validator from 32 ETH to 2,048 ETH. Validators may receive protocol-defined rewards for proposing blocks, attesting to valid blocks and participating in sync committees. Rewards consist of newly issued ETH and transaction-related fees. Transaction fees on Ethereum follow the mechanism introduced by EIP-1559, under which each transaction includes a base fee that is burned at the protocol level and an optional priority fee paid to the validator proposing the relevant block. Validators that engage in certain malicious behaviour, including equivocation or contradictory attestations, may be subject to slashing penalties. Validators that fail to participate correctly in consensus activities may also incur inactivity penalties. These mechanisms are intended to support validator participation and the economic security of the Ethereum network.

Flow's incentive model rewards validator nodes, supports ecosystem growth, and maintains affordable fees for developers and users.

Incentive Mechanisms:

1. Staking Rewards for Specialized Nodes:
   Role-Based Rewards: Validators earn Flow tokens according to their specific roles and contributions within the multi-node architecture, aligning rewards with each node's responsibilities to encourage balanced and effective network participation.
2. Transaction Fees:
   Stable and Consumer-Friendly Fees: Flow's fee structure is designed for predictability, keeping transaction costs stable for both developers and users. Fees are based on transaction complexity and provide an ongoing income stream for validators.
3. Misbehavior Penalties:
   Penalties for Downtime or Malicious Behavior: To maintain network stability, Flow imposes penalties on validators for misbehavior or downtime. This incentivizes high-quality validator participation and ensures consistent performance.
4. Ecosystem and Developer Support:
   Dedicated Portion of Fees and Rewards: A portion of Flow's transaction fees and rewards is allocated to developer initiatives, ecosystem growth, and community engagement. This investment fosters innovation, supports long-term network health, and aligns incentives for ecosystem development.

Hedera Hashgraph incentivizes network participation through transaction fees and staking rewards, with a structured and predictable fee model designed for enterprise use.

Incentive Mechanisms:

1. Staking Rewards for Nodes:
   - HBAR Rewards for Node Operators: Node operators earn HBAR rewards for providing network security and processing transactions, incentivizing them to act honestly and support network stability.
   - User Staking: HBAR holders can stake their tokens to support nodes. Staking rewards offer an additional incentive for token holders to engage in network operations, although the structure may evolve with network growth.
2. Service-Based Node Rewards:
   Nodes receive rewards based on specific services they provide to the network, such as:
   - Consensus Services: Reaching consensus and maintaining transaction order.
   - File Storage: Storing data on the Hedera network.

- Smart Contract Processing: Supporting contract executions for decentralized applications.

Applicable Fees:

1. Predictable Transaction Fees: Hedera's fee structure is fixed and predictable, ensuring transparent costs for users and appealing to enterprise-grade applications. Transaction fees are paid in HBAR and are designed to be stable, making it easier for businesses to plan for usage costs.
2. Fee Allocation: All transaction fees collected in HBAR are distributed to network nodes as rewards, reinforcing their role in maintaining network integrity and processing transactions efficiently.

Hyperliquid incentivizes participants through its native token, HYPE. Validators and delegators earn rewards in HYPE for securing the network and participating in governance. Users can also earn HYPE by staking, providing liquidity, and engaging in other ecosystem activities. This dual-token system encourages active participation and supports the network's growth and stability.

Hyperliquid employs a dynamic fee model where transaction fees are based on network activity and the complexity of the transactions. These fees are paid by users conducting transactions on the network and are designed to cover the costs of processing transactions while incentivizing validators.

Injective incentivizes network participation through staking rewards and a unique transaction fee model that supports long-term value for INJ tokens.

Incentive Mechanisms:

Staking Rewards:
INJ holders earn rewards for staking their tokens, encouraging active participation in securing the network.
Validator Rewards:
Validators receive staking rewards and transaction fees for processing transactions and maintaining network security.

Applicable Fees:

Transaction Fees:
Users pay fees in INJ tokens for network transactions, including smart contract execution and trading.
Fee Structure:
A portion of transaction fees is burned via a weekly on-chain auction, reducing the overall supply of INJ tokens and supporting a deflationary tokenomics model.

Like Ethereum, the Network uses a gas system, where gas is the unit of computational effort required to process a transaction. All gas fees on the Network are paid in Ether (ETH). The Network has a base fee that is designed to stabilize at 7 wei. The base fee still decreases or increases based on network traffic, similar to Ethereum, but it does not go below 7 wei. The Network does not require token staking for transaction validation purposes and thus provides no staking rewards. It does not offer incentives for running a full network node. It does charge fees collected by the sequencer for transaction processing. Those fees are paid in ETH, 20% of which are immediately burned while the remaining 80% are converted to Tokens and then burned.

NEAR Protocol employs several economic mechanisms to secure the network and incentivize participation.

Incentive Mechanisms to Secure Transactions:

1. Staking Rewards:
   Validators and delegators secure the network by staking NEAR tokens. Validators earn around 5% annual inflation, with 90% of newly minted tokens distributed as staking rewards. Validators propose blocks, validate transactions, and receive a share of these rewards based on their staked tokens. Delegators earn rewards proportional to their delegation, encouraging broad participation.
2. Delegation:
   Token holders can delegate their NEAR tokens to validators to increase the validator's stake and improve the chances of being selected to validate transactions. Delegators share in the validator's rewards based on their delegated tokens, incentivizing users to support reliable validators.
3. Slashing and Economic Penalties:
   Validators face penalties for malicious behavior, such as failing to validate correctly or acting dishonestly. The slashing mechanism enforces security by deducting a portion of their staked tokens, ensuring validators follow the network's best interests.
4. Epoch Rotation and Validator Selection:
   Validators are rotated regularly during epochs to ensure fairness and prevent centralization. Each epoch reshuffles validators, allowing the protocol to balance decentralization with performance.

Fees on the NEAR Blockchain:

1. Transaction Fees:
   Users pay fees in NEAR tokens for transaction processing, which are burned to reduce the total circulating supply, introducing a potential deflationary effect over time. Validators also receive a portion of transaction fees as additional rewards, providing an ongoing incentive for network maintenance.
2. Storage Fees:
   NEAR Protocol charges storage fees based on the amount of blockchain storage consumed by accounts, contracts, and data. This requires users to hold NEAR tokens as a deposit proportional to their storage usage, ensuring the efficient use of network resources.
3. Redistribution and Burning:
   A portion of the transaction fees (burned NEAR tokens) reduces the overall supply, while the rest is distributed to validators as compensation for their work. The burning mechanism helps maintain long-term economic sustainability and potential value appreciation for NEAR holders.
4. Reserve Requirement:
   Users must maintain a minimum account balance and reserves for data storage, encouraging efficient use of resources and preventing spam attacks.

Optimism charges lower transaction fees than Ethereum Layer 1, as transactions are bundled in the rollup and written to the Ethereum main chain in compressed form. Gas fees on Optimism continue to be paid in ETH. The incentive model is based on increased efficiency for users (lower fees, faster confirmation) and on the role of sequencers. Sequencers are central actors who collect, organize, and include transactions in the rollup. Their revenue comes from the gas fees they charge.

The network is described as applying transaction fees as a core economic mechanism to support network operation and security. Fee flows may be used to remunerate relevant network roles (for example, sequencer- or validator-related functions, if and to the extent such roles exist in the deployed architecture). In addition, PLUME is described as being used in connection with incentive and participation mechanisms, including potential staking-related arrangements and interaction with DeFi applications. Any yields, rewards, or other economic benefits are contingent on protocol

parameters, market conditions, and user behaviour, and may be changed by governance or technical updates, or may not materialise as expected.

Polygon PoS uses economic incentives to support validator participation, transaction processing, and network operation. Validators stake POL tokens and participate in block production, validation, voting, and checkpoint finalisation. Validators may receive rewards connected to their participation in the network, including rewards linked to validation activities and transaction-fee allocation, depending on the applicable protocol rules. Token holders who do not operate validator infrastructure may delegate POL tokens to validators. Delegators may receive a share of rewards attributable to the validator to whom they delegate, subject to the validator's commission and applicable protocol rules. Delegation increases the validator's effective stake and may affect its role in the validator set and related network processes. Following the Rio upgrade, Polygon PoS introduced a Validator-Elected Block Producer model, under which validators elect the block producer or block producers for a span. Publicly described protocol changes associated with this model also provide for redistribution of fees, including maximum extractable value-related fees where applicable, to non-producing validators under the relevant protocol design. This changes the incentive structure from the previous model in which block production selection was more directly described by reference to stake-weighted producer selection. Polygon PoS includes protocol specifications for validator penalties, including slashing-related concepts. Transactions on Polygon PoS require payment of network fees in POL. Fees apply to ordinary token transfers, smart contract deployment, and smart contract interaction. The amount of fees may vary depending on network demand, transaction complexity, and computational resources required. Because Polygon PoS processes transactions independently from Ethereum, transaction fees are generally designed to be lower than equivalent activity on the Ethereum mainnet, although actual fees may change according to network conditions and protocol parameters.

The Ripple XRP blockchain uses a unique incentive structure that differs from traditional Proof of Work (PoW) or Proof of Stake (PoS) systems, focusing on its Ripple Protocol Consensus Algorithm (RPCA).

Incentive Mechanisms to Secure Transactions:

1. Validators: Validators on the Ripple network are not directly compensated with rewards like in PoW/PoS models. Instead, they are incentivized by the utility and stability of the network, particularly financial institutions that benefit from Ripple's efficiency in cross-border payments.
2. No Mining: Since Ripple does not use mining, it eliminates the need for energy-intensive computations, contributing to fast transaction speeds and scalability.

Fees on the Ripple XRP Blockchain:

1. Transaction Fees: Ripple charges minimal transaction fees (typically fractions of an XRP, known as \drops") for each transaction. The purpose of these fees is to prevent network spam and overload.
2. Burn Mechanism: A portion of each transaction fee is burned, meaning it's permanently removed from circulation. This reduces the overall supply of XRP over time, contributing to potential long-term value stability.

The Sei Network incentivizes participation through staking rewards and a transparent fee structure, supporting its decentralized ecosystem.

Incentive Mechanisms:

- Staking Rewards: Validators and delegators earn SEI tokens as rewards for securing the network through staking, promoting active engagement and long-term commitment.

- Governance Participation: SEI token holders can participate in network governance decisions, influencing protocol upgrades and key changes.

Applicable Fees:

Transaction Fees: Users pay fees in SEI tokens for network transactions. These fees are distributed to validators and delegators as rewards, supporting network operations and security.

Solana uses a combination of Proof of History (PoH) and Proof of Stake (PoS) to secure its network and validate transactions.

Incentive Mechanisms:

1. Validators:
   - Staking Rewards: Validators are chosen based on the number of SOL tokens they have staked. They earn rewards for producing and validating blocks, which are distributed in SOL. The more tokens staked, the higher the chances of being selected to validate transactions and produce new blocks.
   - Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This provides an additional financial incentive for validators to process transactions efficiently and maintain the network's integrity.
2. Delegators:
   - Delegated Staking: Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share in the rewards earned by the validators. This encourages widespread participation in securing the network and ensures decentralization.
3. Economic Security:
   - Slashing: Validators can be penalized for malicious behavior, such as producing invalid blocks or being frequently offline. This penalty, known as slashing, involves the loss of a portion of their staked tokens. Slashing deters dishonest actions and ensures that validators act in the best interest of the network.
   - Opportunity Cost: By staking SOL tokens, validators and delegators lock up their tokens, which could otherwise be used or sold. This opportunity cost incentivizes participants to act honestly to earn rewards and avoid penalties. Fees Applicable on the Solana Blockchain

Transaction Fees:

1. Low and Predictable Fees:
   Solana is designed to handle a high throughput of transactions, which helps keep fees low and predictable. The average transaction fee on Solana is significantly lower compared to other blockchains like Ethereum.
2. Fee Structure:
   Fees are paid in SOL and are used to compensate validators for the resources they expend to process transactions. This includes computational power and network bandwidth.
3. Rent Fees:
   State Storage: Solana charges rent fees for storing data on the blockchain. These fees are designed to discourage inefficient use of state storage and encourage developers to clean up unused state. Rent fees help maintain the efficiency and performance of the network.
4. Smart Contract Fees:
   Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This ensures that users are charged proportionally for the resources they consume.

Sonic's economic model is designed to incentivize active participation from both validators and developers. Validators earn rewards through a combination of block rewards and transaction fees. The block reward system employs a dynamic Annual Percentage Rate (APR) mechanism.

Starknet's incentive model combines transaction fees and plans for future staking rewards to support network operations and security.

Incentive Mechanisms:

- Transaction Fees: Users pay fees in Ether (ETH) to compensate sequencers and cover the cost of proof submission and storage on Ethereum.
- Dynamic Fee Model: Fees adjust based on transaction complexity and resource requirements, ensuring fair cost distribution and efficient network usage.
- Future Staking Rewards: Planned staking mechanisms will incentivize participants to lock their STARK tokens, enhancing network security and governance.

Statemint is a common-good parachain on the Polkadot and Kusama networks, designed to enable efficient asset management while benefiting from Polkadot's shared security and governance model.

Incentive Mechanisms:

- Relay Chain Validators: Validators securing the Polkadot Relay Chain are indirectly incentivized through block rewards and transaction fees collected across all parachains, including Statemint. This ensures the stability and security of the network without requiring Statemint-specific rewards.
- Collator Compensation: Collator nodes aggregate transactions and produce blocks for Statemint. They may be compensated through external arrangements, such as subsidies or user-driven incentives, depending on governance decisions and usage patterns.
- Governance Participation: Polkadot (DOT) and Kusama (KSM) token holders influence Statemint's operations, such as fee adjustments and protocol upgrades, through on-chain governance mechanisms.

Applicable Fees:

- Transaction Fees: Users pay transaction fees in the native tokens of the Relay Chain, DOT for Polkadot or KSM for Kusama. These fees are distributed to Relay Chain validators to support the network's maintenance.
- Asset Creation and Transfer Fees: Fees apply for creating new assets and transferring them on the Statemint chain. These fees help prevent spam and ensure efficient use of network resources.
- Governance-Defined Fee Adjustments: The Statemint parachain's fees can be adjusted through governance proposals, enabling the community to adapt costs to network conditions.

Stellar does not use block rewards or mining. Instead, validators operate without direct protocol-level rewards. While this design keeps costs low, it may reduce incentives for validator participation compared to staking-based models. The sustainability of validator engagement depends largely on external factors such as institutional involvement and ecosystem adoption.

Security and Economic Incentives:

1. Validators:
   Validators stake SUI tokens to participate in the consensus process. They earn rewards for validating transactions and securing the network.

2. Slashing:
   Validators can be penalized (slashed) for malicious behavior, such as double-signing or failing to properly validate transactions. This helps maintain network security and incentivizes honest behavior.
3. Delegation:
   Token holders can delegate their SUI tokens to trusted validators. In return, they share in the rewards earned by validators. This encourages widespread participation in securing the network.

Fees on the SUI Blockchain:

1. Transaction Fees:
   Users pay transaction fees to validators for processing and confirming transactions. These fees are calculated based on the computational resources required to process the transaction. Fees are paid in SUI tokens, which is the native cryptocurrency of the Sui blockchain.
2. Dynamic Fee Model:
   The transaction fees on Sui are dynamic, meaning they adjust based on network demand and the complexity of the transactions being processed.

The Tron blockchain uses a Delegated Proof of Stake (DPoS) consensus mechanism to secure its network and incentivize participation.

Incentive Mechanism:

1. Super Representatives (SRs) Rewards:
   - Block Rewards: Super Representatives (SRs), who are elected by TRX holders, are rewarded for producing blocks. Each block they produce comes with a block reward in the form of TRX tokens.
   - Transaction Fees: In addition to block rewards, SRs receive transaction fees for validating transactions and including them in blocks. This ensures they are incentivized to process transactions efficiently.
2. Voting and Delegation:
   - TRX Staking: TRX holders can stake their tokens and vote for Super Representatives (SRs). When TRX holders vote, they delegate their voting power to SRs, which allows SRs to earn rewards in the form of newly minted TRX tokens.
   - Delegator Rewards: Token holders who delegate their votes to an SR can also receive a share of the rewards. This means delegators share in the block rewards and transaction fees that the SR earns.
   - Incentivizing Participation: The more tokens a user stakes, the more voting power they have, which encourages participation in governance and network security.
3. Incentive for SRs:
   SRs are also incentivized to maintain the health and performance of the network. Their reputation and continued election depend on their ability to produce blocks consistently and efficiently process transactions.

Applicable Fees:

1. Transaction Fees:
   - Fee Calculation: Users must pay transaction fees to have their transactions processed. The transaction fee varies based on the complexity of the transaction and the network's current demand. This is paid in TRX tokens. Transaction
   - Fee Distribution: Transaction fees are distributed to Super Representatives (SRs), giving them an ongoing income to maintain and support the network.

2. Storage Fees:
   Tron charges storage fees for data storage on the blockchain. This includes storing smart contracts, tokens, and other data on the network. Users are required to pay these fees in TRX tokens to store data.
3. Energy and Bandwidth:
   Energy: Tron uses a resource model that allows users to access network resources like bandwidth and energy through staking. Users who stake their TRX tokens receive \energy

XinFin incentivizes both validators and token holders to actively participate in network security and stability through staking and fee distribution mechanisms.

Incentive Mechanisms:

1. Staking Rewards:
   - Validator Rewards: Validators earn XDC token rewards for validating transactions and maintaining network security.
   - Delegator Rewards: XDC holders who delegate their tokens to validators receive a share of staking rewards, promoting community participation without requiring users to operate nodes.
2. Delegation Model:
   Passive Income: XDC holders can delegate tokens to validators, enabling them to earn rewards passively and boosting network security through broader staking participation.

Applicable Fees:

- Fee Distribution: All transactions incur XDC fees, which are distributed to validators as additional rewards for their role in securing the network.
- Predictable Fees for Enterprises: Transaction fees are kept low and predictable, supporting XinFin's focus on enterprise use cases in finance, trade, and cross-border payments.

zkSync incentivizes network participants through a streamlined fee structure and role-based rewards, designed to ensure security, scalability, and usability for both users and validators.

Incentive Mechanism:

- Validator Rewards: Validators, who generate validity proofs and secure the network, are compensated through transaction fees paid by users. Their role ensures that batches of transactions are processed efficiently and accurately.
- Sequencer Incentives: Sequencers are responsible for bundling and ordering transactions off-chain. They earn a share of the transaction fees for maintaining network performance and fast processing times.
- Ecosystem Growth Rewards: zkSync allocates resources to incentivize developers and projects building on its platform, fostering a robust ecosystem of dApps, DeFi protocols, and NFT marketplaces.

Applicable Fees:

- Transaction Fees: Users pay fees in Ether (ETH) for transactions on zkSync. These fees are significantly lower than Ethereum Layer 1 fees, as zkSync processes transactions off-chain and submits only aggregated proofs to the Ethereum mainnet.
- Fee Model: Fees are dynamically calculated based on the complexity of transactions (e.g., token transfers, smart contract interactions) and the cost of submitting validity proofs to Ethereum.
- Scalability Benefits: zkSync's efficient rollup architecture reduces gas fees for users while ensuring that validators and sequencers are appropriately compensated for their roles.

S.9 Energy consumption sources and methodologies

The energy consumption of this asset is aggregated across multiple components:

To determine the energy consumption of a token, the energy consumption of the network(s) algorand, aptos_coin, arbitrum, avalanche, base, celo, ethereum, flow, hedera_hbar, hyperliquid, injective, linea, near_protocol, optimism, plume, polygon, ripple, sei, solana, sonic, starknet, statemint, stellar, sui, tron, xdc_network, zksync is calculated first. For the energy consumption of the token, a fraction of the energy consumption of the network is attributed to the token, which is determined based on the activity of the crypto-asset within the network. When calculating the energy consumption, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used - if available - to determine all implementations of the asset in scope. The mappings are updated regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

Bitcoin Liquid

LBTC | M3NCNSV6B

Quantitative information

Quantitative sustainability indicators for Bitcoin Liquid

Field	Value	Unit
S.1 Name	STOKR S.A.	/
S.2 Relevant legal entity identifier	984500BA521C5EMR1D63	/
S.3 Name of the crypto-asset	Bitcoin Liquid	/
S.6 Beginning of the period to which the disclosure relates	2025-09-11	/
S.7 End of the period to which the disclosure relates	2026-09-11	/
S.8 Energy consumption	15373.80000	kWh/a

Qualitative information

S.4 Consensus Mechanism

The Liquid Network is a Layer 2 solution on Bitcoin designed for fast, confidential transactions and asset issuance, secured by a federated model called Strong Federations. Instead of using Bitcoin's Proof of Work, the Liquid Network relies on trusted functionaries for consensus.

Core Components:

1. Federated Model:
   Trusted Functionaries: The Liquid Network is secured by a group of trusted entities, such as exchanges and financial institutions, called functionaries. This model provides faster transaction speeds by limiting consensus to a small, trusted group.
2. Role of Functionaries:
   - Block Signers: Functionaries are responsible for validating transactions and creating blocks. Blocks are confirmed when two-thirds of functionaries sign, ensuring secure and quick consensus.
   - Watchmen: Functionaries responsible for overseeing the peg-in and peg-out process between Bitcoin and the Liquid Network, ensuring that Liquid Bitcoin (L-BTC) is always backed by real Bitcoin.
3. Block Creation and Validation:
   - Regular Block Intervals: Blocks are produced every minute without mining, relying on multi-signature validation by block signers.
   - Multi-Signature Approval: At least two-thirds of block signers must validate and sign each block, preventing any single entity from controlling block production.

4. Peg-in and Peg-out Mechanism:
   - Peg-in Process: Users move Bitcoin onto the Liquid Network by sending it to a multi-signature address. In return, an equivalent amount of L-BTC is issued.
   - Peg-out Process: To move Bitcoin back to the Bitcoin blockchain, users initiate a peg-out, where Watchmen release the corresponding Bitcoin.
5. Confidential Transactions:
   Privacy with Confidential Transactions (CT): Liquid uses CT to hide transaction amounts, ensuring privacy while allowing functionaries to verify transaction validity. This feature is essential for financial institutions and users who require privacy.

S.5 Incentive Mechanisms and Applicable Fees

Liquid's federated model incentivizes functionaries to maintain network security, with transaction fees as the primary source of income for network operations and validator rewards.

Incentive Mechanisms:

- Transaction Fees: User-Paid Fees: Each transaction on the Liquid Network incurs a fee paid in L-BTC. These fees are awarded to functionaries (specifically block signers), providing an incentive to validate and maintain the network

Applicable Fees:

- Transaction Fees: Minimal Transaction Costs: Fees on the Liquid Network are generally low, encouraging high-volume transactions.
- Confidential Transaction Costs: Confidential Transactions, while private, may incur slightly higher fees due to additional cryptographic processes.

S.9 Energy consumption sources and methodologies

For the calculation of energy consumptions, the so called 'bottom-up' approach is being used. The nodes are considered to be the central factor for the energy consumption of the network. These assumptions are made on the basis of empirical findings through the use of public information sites, open-source crawlers and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the client software. The energy consumption of the hardware devices was measured in certified test laboratories. Due to the structure of this network, it is not only the mainnet that is responsible for energy consumption. In order to calculate the structure adequately, a proportion of the energy consumption of the connected network, bitcoin, must also be taken into account, because the connected network is also responsible for security. This proportion is determined on the basis of gas consumption. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset of question in scope and we update the mappings regulary, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

Quantoz USDQ

USDQ | XL2ZV90NC

Quantitative information

Quantitative sustainability indicators for Quantoz USDQ

Field	Value	Unit
S.1 Name	STOKR S.A.	/
S.2 Relevant legal entity identifier	984500BA521C5EMR1D63	/
S.3 Name of the crypto-asset	Quantoz USDQ	/
S.6 Beginning of the period to which the disclosure relates	2025-09-11	/
S.7 End of the period to which the disclosure relates	2026-09-11	/
S.8 Energy consumption	118.41035	kWh/a

Qualitative information

S.4 Consensus Mechanism

Quantoz USDQ is present on the following networks: Algorand, Ethereum, Polygon.

The Algorand blockchain utilizes a consensus mechanism termed Pure Proof-of-Stake (PPoS). Consensus, in this context, describes the method by which blocks are selected and appended to the blockchain. Algorand employs a verifiable random function (VRF) to select leaders who propose blocks for each round.

Upon block proposal, a pseudorandomly selected committee of voters is chosen to evaluate the proposal. If a supermajority of these votes are from honest participants, the block is certified. What makes this algorithm a Pure Proof of Stake is that users are chosen for committees based on the number of algos in their accounts. This system leverages random committee selection to maintain high performance and inclusivity within the network.

The consensus process involves three stages:

1. Propose: A leader proposes a new block.
2. Soft Vote: A committee of voters assesses the proposed block.
3. Certify Vote: Another committee certifies the block if it meets the required honesty threshold.

Ethereum uses a Proof-of-Stake (PoS) consensus mechanism introduced with The Merge on 2022-09-15, which replaced the previous Proof-of-Work consensus model. The PoS mechanism is implemented through Gasper, combining Casper-FFG for finality with the LMD-GHOST fork-choice rule for chain selection. Validators participate in consensus by staking ETH through the Beacon Chain. Validators are pseudo-randomly selected to propose new blocks, while other validators attest

to the validity of proposed blocks. The network operates using 12-second slots grouped into epochs of 32 slots. Under normal network conditions, finality is typically achieved after two epochs, approximately 12.8 minutes, through Casper-FFG. The LMD-GHOST fork-choice rule determines the canonical chain based on the accumulated weight of validator attestations. Validators that engage in certain malicious behaviour, such as equivocation or contradictory attestations, may be subject to slashing penalties, while offline validators may incur inactivity penalties. Subsequent network upgrades, including Dencun (2024-03-13), Pectra (2025-05-07) and Fusaka (2025-12-03), introduced protocol changes affecting Ethereum's consensus mechanism and Layer 2 functionality.

Polygon PoS is an EVM-compatible sidechain that operates with a Proof-of-Stake consensus mechanism and periodically submits checkpoints to the Ethereum mainnet. The network maintains its own validator set and processes transactions independently from Ethereum, while using Ethereum smart contracts for staking-related functions and checkpoint verification. Polygon PoS therefore uses Ethereum as a staking and checkpointing layer, but does not rely on Ethereum for full transaction execution or transaction data availability. The Polygon-side architecture consists of two primary node layers. The Bor layer is responsible for transaction execution and block production. The Heimdall layer is responsible for validator coordination, staking-related monitoring, consensus, and checkpoint finalisation. Heimdall is based on Cosmos SDK and CometBFT and aggregates blocks produced by Bor into periodic Merkle-root checkpoints that are submitted to smart contracts on the Ethereum mainnet. Validators participate in the network by staking POL tokens. Token holders may delegate POL tokens to validators, contributing to the validator's effective stake and participating indirectly in network validation. Following the Rio upgrade, Polygon PoS uses a Validator-Elected Block Producer model. Under this model, validators elect the block producer or block producers for a span, rather than relying on the previous stake-weighted selection model for multiple block producers over shorter intervals. Block production and transaction execution are performed on the Bor layer, while Heimdall validators coordinate consensus and checkpoint finalisation. At regular intervals, Heimdall validators aggregate blocks into a Merkle root and submit the resulting checkpoint to Ethereum smart contracts. These checkpoints provide an additional verification layer and support cross-chain verification, including in the context of asset transfers between Polygon PoS and Ethereum. This design enables higher transaction throughput and lower transaction costs than the Ethereum mainnet, while maintaining a technical connection to Ethereum through staking contracts and periodic checkpointing. Polygon PoS should therefore be understood as an independent sidechain or commit-chain architecture, rather than a rollup that inherits full execution and data availability security from Ethereum.

S.5 Incentive Mechanisms and Applicable Fees

Quantoz USDQ is present on the following networks: Algorand, Ethereum, Polygon.

Algorand's consensus mechanism, Pure Proof-of-Stake (PPoS), relies on the participation of token holders (stakers) to ensure the network's security and integrity:

1. Participation Rewards:
   - Staking Rewards: Users who participate in the consensus protocol by staking their ALGO tokens earn rewards. These rewards are distributed periodically and are proportional to the amount of ALGO staked. This incentivizes users to hold and stake their tokens, contributing to network security and stability.
   - Node Participation Rewards: Validators, also known as participation nodes, are responsible for proposing and voting on blocks. These nodes receive additional rewards for their active role in maintaining the network.

2. Transaction Fees:
   - Flat Fee Model: Algorand employs a flat fee model for transactions, which ensures predictability and simplicity. The standard transaction fee on Algorand is very low (around 0.001 ALGO per transaction). These fees are paid by users to have their transactions processed and included in a block.
   - Fee Redistribution: Collected transaction fees are redistributed to participants in the network. This includes stakers and validators, further incentivizing their participation and ensuring continuous network operation.
3. Economic Security:
   Token Locking: To participate in the consensus mechanism, users must lock up their ALGO tokens. This economic stake acts as a security deposit that can be slashed (forfeited) if the participant acts maliciously. The potential loss of staked tokens discourages dishonest behavior and helps maintain network integrity.

Fees on the Algorand Blockchain

1. Transaction Fees:
   Algorand uses a flat transaction fee model. The current standard fee is 0.001 ALGO per transaction. This fee is minimal compared to other blockchain networks, ensuring affordability and accessibility.
2. Smart Contract Execution Fees:
   Fees for executing smart contracts on Algorand are also designed to be low. These fees are based on the computational resources required to execute the contract, ensuring that users are only charged for the actual resources they consume.
3. Asset Creation Fees:
   Creating new assets (tokens) on the Algorand blockchain involves a small fee. This fee is necessary to prevent spam and ensure that only genuine assets are created and maintained on the network.

Ethereum's Proof-of-Stake (PoS) mechanism secures the network through validator incentives and protocol-defined penalties. Validators are required to stake ETH in order to participate in block proposal and attestation activities. A minimum of 32 ETH is required to activate a validator. Following the Pectra upgrade on 2025-05-07, EIP-7251 increased the maximum effective balance per validator from 32 ETH to 2,048 ETH. Validators may receive protocol-defined rewards for proposing blocks, attesting to valid blocks and participating in sync committees. Rewards consist of newly issued ETH and transaction-related fees. Transaction fees on Ethereum follow the mechanism introduced by EIP-1559, under which each transaction includes a base fee that is burned at the protocol level and an optional priority fee paid to the validator proposing the relevant block. Validators that engage in certain malicious behaviour, including equivocation or contradictory attestations, may be subject to slashing penalties. Validators that fail to participate correctly in consensus activities may also incur inactivity penalties. These mechanisms are intended to support validator participation and the economic security of the Ethereum network.

Polygon PoS uses economic incentives to support validator participation, transaction processing, and network operation. Validators stake POL tokens and participate in block production, validation, voting, and checkpoint finalisation. Validators may receive rewards connected to their participation in the network, including rewards linked to validation activities and transaction-fee allocation, depending on the applicable protocol rules. Token holders who do not operate validator infrastructure may delegate POL tokens to validators. Delegators may receive a share of rewards attributable to the validator to whom they delegate, subject to the validator's commission and applicable protocol rules. Delegation increases the validator's effective stake and may affect its role in the validator set and related network processes. Following the Rio upgrade, Polygon PoS introduced

a Validator-Elected Block Producer model, under which validators elect the block producer or block producers for a span. Publicly described protocol changes associated with this model also provide for redistribution of fees, including maximum extractable value-related fees where applicable, to non-producing validators under the relevant protocol design. This changes the incentive structure from the previous model in which block production selection was more directly described by reference to stake-weighted producer selection. Polygon PoS includes protocol specifications for validator penalties, including slashing-related concepts. Transactions on Polygon PoS require payment of network fees in POL. Fees apply to ordinary token transfers, smart contract deployment, and smart contract interaction. The amount of fees may vary depending on network demand, transaction complexity, and computational resources required. Because Polygon PoS processes transactions independently from Ethereum, transaction fees are generally designed to be lower than equivalent activity on the Ethereum mainnet, although actual fees may change according to network conditions and protocol parameters.

S.9 Energy consumption sources and methodologies

The energy consumption of this asset is aggregated across multiple components:

To determine the energy consumption of a token, the energy consumption of the network(s) algorand, ethereum, polygon is calculated first. For the energy consumption of the token, a fraction of the energy consumption of the network is attributed to the token, which is determined based on the activity of the crypto-asset within the network. When calculating the energy consumption, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used - if available - to determine all implementations of the asset in scope. The mappings are updated regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

This report was provided by:

Crypto Risk Metrics

Our services

ESG data for crypto-assets

Provision of ESG data for crypto-assets in compliance with MiCA requirements. The data is based on ISO-certified measurements, is legally robust, can be easily integrated, and is trusted by leading regulated market participants operating in different regulatory environments.

White papers for crypto-assets

Crypto Risk Metrics supports CASPs in drafting and maintaining MiCA-compliant white papers, including ESG disclosures, or assumes responsibility for the entire process through its "White Glove Service", with transfer of liability. If the issuer of the crypto-asset does not provide a white paper, the trading platform may prepare and submit it to the competent authority.

Risk management

Crypto Risk Metrics provides a MaRisk- and BAIT-compliant SaaS solution that helps financial institutions manage risks in direct and indirect crypto-asset investments by reference to BSI standards and other recognised standards. Daily reports and a complete audit trail ensure transparent, audit-ready documentation of crypto-asset risks.

Compliant price data

Crypto Risk Metrics delivers KARBV-compliant price data for native crypto-assets using a valuation model tailored to non-organised markets, such as Bitcoin and Ethereum. This ensures accurate asset valuation in line with Sections 27 and 28 of the German Investment Accounting and Valuation Ordinance (KARBV).

Market conformity check

The service ensures compliance with Circular 05/2023 (BA) through automated verification of the market conformity of crypto trades and by flagging potentially non-conforming transactions. Customers receive daily trade reports securely via SFTP or in CSV format, simplifying regulatory risk management.

Contact

Crypto Risk Metrics GmbH
Lange Reihe 73
20099 Hamburg
Germany

Tel.: +49 251 981156-4070
Mail: info@crypto-risk-metrics.com