

BVNK

Sustainability indicators for USDC

Disclosures in accordance with
Article 66 (5) MiCAR.



This report was provided by Crypto Risk Metrics.

2025-11-19

Preamble

About the Crypto Asset Service Provider (CASP)

Name of the CASP: System Pay Services (Malta) Limited
Street and number: TRQ SANT'ANDRIJA, Malta
City: SAN GILJAN
Country: Malta
LEI: 984500640Z8ADE893D04


About this report

This disclosure serves as evidence of compliance with the regulatory requirements of MiCAR 66 (5). This requirement obliges crypto asset service providers to disclose significant adverse factors affecting the climate and the environment. In particular, this disclosure complies with the requirements of “Commission Regulation (EU) 2025/422 of December 17, 2024, supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content, methods and presentation of information relating to sustainability indicators related to climate-related and other environmental impacts.” The optional information specified in Article 6, par. 8 (a) to (d) DR 2025/422 is not included.

This report is valid until material changes occur in the data, which will result in an immediate adjustment of this report.

Sustainability indicators

USDC



Quantitative information

Field	Value	Unit
S.1 Name	System Pay Services (Malta) Limited	/
S.2 Relevant legal entity identifier	984500640Z8ADE893D04	/
S.3 Name of the crypto-asset	USDC	/
S.6 Beginning of the period to which the disclosure relates	2024-11-19	/
S.7 End of the period to which the disclosure relates	2025-11-19	/
S.8 Energy consumption	552504.11932	kWh/a
S.10 Renewable energy consumption	37.4403637777	%
S.11 Energy intensity	0.00001	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	194.27699	tCO2e
S.14 GHG intensity	0.00000	kgCO2e

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, Linea, Near Protocol, Optimism, Plume, Polygon, Ripple, Sei, Solana, Sonic, 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 a Layer 2 solution on top of Ethereum that uses Optimistic Rollups to enhance scalability and reduce transaction costs. It assumes that transactions are valid by default and only verifies them if there's a challenge (optimistic).

Core Components:

- Sequencer: Orders transactions and creates batches for processing.
- Bridge: Facilitates asset transfers between Arbitrum and Ethereum.
- Fraud Proofs: Protect against invalid transactions through an interactive verification process.

Verification Process:

1. Transaction Submission: Users submit transactions to the Arbitrum Sequencer, which orders and batches them.
2. State Commitment: These batches are submitted to Ethereum with a state commitment.
3. Challenge Period: Validators have a specific period to challenge the state if they suspect fraud.

4. Dispute Resolution: If a challenge occurs, the dispute is resolved through an iterative process to identify the fraudulent transaction. The final operation is executed on Ethereum to determine the correct state.
5. Rollback and Penalties: If fraud is proven, the state is rolled back, and the dishonest party is penalized.

Security and Efficiency: The combination of the Sequencer, bridge, and interactive fraud proofs ensures that the system remains secure and efficient. By minimizing on-chain data and leveraging off-chain computations, Arbitrum can provide high throughput and low fees.

The Avalanche blockchain network employs a unique Proof-of-Stake consensus mechanism called Avalanche Consensus, which involves three interconnected protocols: Snowball, Snowflake, and Avalanche.

Avalanche Consensus Process:

1. Snowball Protocol:
 - Random Sampling: Each validator randomly samples a small, constant-sized subset of other validators.
 - Repeated Polling: Validators repeatedly poll the sampled validators to determine the preferred transaction.
 - Confidence Counters: Validators maintain confidence counters for each transaction, incrementing them each time a sampled validator supports their preferred transaction.
 - Decision Threshold: Once the confidence counter exceeds a pre-defined threshold, the transaction is considered accepted.
2. Snowflake Protocol:
 - Binary Decision: Enhances the Snowball protocol by incorporating a binary decision process. Validators decide between two conflicting transactions.
 - Binary Confidence: Confidence counters are used to track the preferred binary decision.
 - Finality: When a binary decision reaches a certain confidence level, it becomes final.
3. Avalanche Protocol:
 - DAG Structure: Uses a Directed Acyclic Graph (DAG) structure to organize transactions, allowing for parallel processing and higher throughput.
 - Transaction Ordering: Transactions are added to the DAG based on their dependencies, ensuring a consistent order.
 - Consensus on DAG: While most Proof-of-Stake Protocols use a Byzantine Fault Tolerant (BFT) consensus, Avalanche uses the Avalanche Consensus, Validators reach consensus on the structure and contents of the DAG through repeated Snowball and Snowflake.

Base is a Layer-2 (L2) solution on Ethereum that was introduced by Coinbase and developed using Optimism's OP Stack. L2 transactions do not have their own consensus mechanism and are only validated by the execution clients. The so-called sequencer regularly bundles stacks of L2 transactions and publishes them on the L1 network, i.e. Ethereum. Ethereum's consensus mechanism (Proof-of-stake) thus indirectly secures all L2 transactions as soon as they are written to L1.

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.

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity.

The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

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.

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 DooMLug, 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.

Optimism is a Layer 2 scaling solution for Ethereum that uses Optimistic Rollups to increase transaction throughput and reduce costs while inheriting the security of the Ethereum main chain.

Core Components:

1. Optimistic Rollups:

- Rollup Blocks: Transactions are batched into rollup blocks and processed off-chain.
- State Commitments: The state of these transactions is periodically committed to the Ethereum main chain.

2. Sequencers:

- Transaction Ordering: Sequencers are responsible for ordering transactions and creating batches.
- State Updates: Sequencers update the state of the rollup and submit these updates to the Ethereum main chain.
- Block Production: They construct and execute Layer 2 blocks, which are then posted to Ethereum.

3. Fraud Proofs:

- Assumption of Validity: Transactions are assumed to be valid by default.
- Challenge Period: A specific time window during which anyone can challenge a transaction by submitting a fraud proof.
- Dispute Resolution: If a transaction is challenged, an interactive verification game is played to determine its validity. If fraud is detected, the invalid state is rolled back, and the dishonest participant is penalized.

Consensus Process:

1. Transaction Submission: Users submit transactions to the sequencer, which orders them into batches.

2. Batch Processing: The sequencer processes these transactions off-chain, updating the Layer 2 state.

3. State Commitment: The updated state and the batch of transactions are periodically committed to the Ethereum main chain. This is done by posting the state root (a cryptographic hash representing the state) and transaction data as calldata on Ethereum.

4. Fraud Proofs and Challenges: Once a batch is posted, there is a challenge period during which anyone can submit a fraud proof if they believe a transaction is invalid.

- Interactive Verification: The dispute is resolved through an interactive verification game, which involves breaking down the transaction into smaller steps to identify the exact point of fraud.

- Rollbacks and Penalties: If fraud is proven, the batch is rolled back, and the dishonest actor loses their staked collateral as a penalty.
5. Finality: After the challenge period, if no fraud proof is submitted, the batch is considered final. This means the transactions are accepted as valid, and the state updates are permanent.

Polygon, formerly known as Matic Network, is a Layer 2 scaling solution for Ethereum that employs a hybrid consensus mechanism. Here's a detailed explanation of how Polygon achieves consensus:

Core Concepts:

1. Proof of Stake (PoS):

- Validator Selection: Validators on the Polygon network are selected based on the number of MATIC 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 who do not wish to run a validator node can delegate their MATIC tokens to validators. Delegators share in the rewards earned by validators.

2. Plasma Chains:

- Off-Chain Scaling: Plasma is a framework for creating child chains that operate alongside the main Ethereum chain. These child chains can process transactions off-chain and submit only the final state to the Ethereum main chain, significantly increasing throughput and reducing congestion.
- Fraud Proofs: Plasma uses a fraud-proof mechanism to ensure the security of off-chain transactions. If a fraudulent transaction is detected, it can be challenged and reverted.

Consensus Process:

1. Transaction Validation:

Transactions are first validated by validators who have staked MATIC tokens. These validators confirm the validity of transactions and include them in blocks.

2. Block Production:

- Proposing and Voting: Validators propose new blocks based on their staked tokens and participate in a voting process to reach consensus on the next block. The block with the majority of votes is added to the blockchain.
- Checkpointing: Polygon uses periodic checkpointing, where snapshots of the Polygon sidechain are submitted to the Ethereum main chain. This process ensures the security and finality of transactions on the Polygon network.

3. Plasma Framework:

- Child Chains: Transactions can be processed on child chains created using the Plasma framework. These transactions are validated off-chain and only the final state is submitted to the Ethereum main chain.
- Fraud Proofs: If a fraudulent transaction occurs, it can be challenged within a certain period using fraud proofs. This mechanism ensures the integrity of off-chain transactions.

Security and Economic Incentives:

1. Incentives for Validators:

- Staking Rewards: Validators earn rewards for staking MATIC tokens and participating in the consensus process. These rewards are distributed in MATIC tokens and are proportional to the amount staked and the performance of the validator.
- Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This provides an additional financial incentive to maintain the network's integrity and efficiency.

2. Delegation:

Shared Rewards: Delegators earn a share of the rewards earned by the validators they delegate to. This encourages more token holders to participate in securing the network by choosing reliable validators.

3. Economic Security:

Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. This penalty, known as slashing, involves the loss of a portion of their staked tokens, ensuring that validators act in the best interest of the network.

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.

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.

Stellar uses a unique consensus mechanism known as the Stellar Consensus Protocol (SCP).

Core Concepts:

1. Federated Byzantine Agreement (FBA):

- SCP is built on the principles of Federated Byzantine Agreement (FBA), which allows decentralized, leaderless consensus without the need for a closed system of trusted participants.
- Quorum Slices: Each node in the network selects a set of other nodes (quorum slice) that it trusts. Consensus is achieved when these slices overlap and collectively agree on the transaction state.

2. Nodes and Validators:

- Nodes: Nodes running the Stellar software participate in the network by validating transactions and maintaining the ledger.
- Validators: Nodes that are responsible for validating transactions and reaching consensus on the state of the ledger.

3. Transaction Validation:

Transactions are submitted to the network and nodes validate them based on predetermined rules, such as sufficient balances and valid signatures.

4. Nomination Phase:

- Nomination: Nodes nominate values (proposed transactions) that they believe should be included in the next ledger. Nodes communicate their nominations to their quorum slices.
- Agreement on Nominations: Nodes vote on the nominated values, and through a process of voting and federated agreement, a set of candidate values emerges. This phase continues until nodes agree on a single value or a set of values.

5. Ballot Protocol (Voting and Acceptance): Balloting:

- The agreed-upon values from the nomination phase are then put into ballots. Each ballot goes through multiple rounds of voting, where nodes vote to either accept or reject the proposed values.
- Federated Voting: Nodes exchange votes within their quorum slices, and if a value receives sufficient votes across overlapping slices, it moves to the next stage.
- Acceptance and Confirmation: If a value gathers enough votes through multiple stages (prepare, confirm, externalize), it is accepted and externalized as the next state of the ledger.

6. Ledger Update:

Once consensus is reached, the new transactions are recorded in the ledger. Nodes update their copies of the ledger to reflect the new state. Security and Economic Incentives

7. Trust and Quorum Slices:

Nodes are free to choose their own quorum slices, which provides flexibility and decentralization. The overlapping nature of quorum slices ensures that the network can reach consensus even if some nodes are faulty or malicious.

8. Stability and Security:

SCP ensures that the network can achieve consensus efficiently without relying on energy-intensive mining processes. This makes it environmentally friendly and suitable for high-throughput applications.

9. Incentive Mechanisms:

Unlike Proof of Work (PoW) or Proof of Stake (PoS) systems, Stellar does not rely on direct economic incentives like mining rewards. Instead, the network incentivizes participation through the intrinsic value of maintaining a secure, efficient, and reliable payment network.

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 fees for 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, Linea, Near Protocol, Optimism, Plume, Polygon, Ripple, Sei, Solana, Sonic, 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.

Arbitrum One, a Layer 2 scaling solution for Ethereum, employs several incentive mechanisms to ensure the security and integrity of transactions on its network. The key mechanisms include:

1. Validators and Sequencers:

- Sequencers are responsible for ordering transactions and creating batches that are processed off-chain. They play a critical role in maintaining the efficiency and throughput of the network.
- Validators monitor the sequencers' actions and ensure that transactions are processed correctly. Validators verify the state transitions and ensure that no invalid transactions are included in the batches.

2. Fraud Proofs:

- Assumption of Validity: Transactions processed off-chain are assumed to be valid. This allows for quick transaction finality and high throughput.
- Challenge Period: There is a predefined period during which anyone can challenge the validity of a transaction by submitting a fraud proof. This mechanism acts as a deterrent against malicious behavior.
- Dispute Resolution: If a challenge is raised, an interactive verification process is initiated to pinpoint the exact step where fraud occurred. If the challenge is valid, the fraudulent transaction is reverted, and the dishonest actor is penalized.

3. Economic Incentives:

- Rewards for Honest Behavior: Participants in the network, such as validators and sequencers, are incentivized through rewards for performing their duties honestly and efficiently. These rewards come from transaction fees and potentially other protocol incentives.
- Penalties for Malicious Behavior: Participants who engage in dishonest behavior or submit invalid transactions are penalized. This can include slashing of staked tokens or other forms of economic penalties, which serve to discourage malicious actions.

Fees on the Arbitrum One Blockchain

1. Transaction Fees:

- Layer 2 Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are typically lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
- Arbitrum Transaction Fee: A fee is charged for each transaction processed by the sequencer. This fee covers the cost of processing the transaction and ensuring its inclusion in a batch.

2. L1 Data Fees:

- Posting Batches to Ethereum: Periodically, the state updates from the Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee, known as the L1 data fee, which accounts for the gas required to publish these state updates on Ethereum.
- Cost Sharing: Because transactions are batched, the fixed costs of posting state updates to Ethereum are spread across multiple transactions, making it more cost-effective for users.

Avalanche uses a consensus mechanism known as Avalanche Consensus, which relies on a combination of validators, staking, and a novel approach to consensus to ensure the network's security and integrity.

1. Validators:

Staking: Validators on the Avalanche network are required to stake AVAX tokens. The amount staked influences their probability of being selected to propose or validate new blocks.

Rewards: Validators earn rewards for their participation in the consensus process. These rewards are proportional to the amount of AVAX staked and their uptime and performance in validating transactions.

Delegation: Validators can also accept delegations from other token holders. Delegators share in the rewards based on the amount they delegate, which incentivizes smaller holders to participate indirectly in securing the network.

2. Economic Incentives:

Block Rewards: Validators receive block rewards for proposing and validating blocks. These rewards are distributed from the network's inflationary issuance of AVAX tokens.

Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This includes fees for simple transactions, smart contract interactions, and the creation of new assets on the network.

3. Penalties:

- Slashing: Unlike some other PoS systems, Avalanche does not employ slashing (i.e., the confiscation of staked tokens) as a penalty for misbehavior. Instead, the network relies on the financial disincentive of lost future rewards for validators who are not consistently online or act maliciously.

- Uptime Requirements: Validators must maintain a high level of uptime and correctly validate transactions to continue earning rewards. Poor performance or malicious actions result in missed rewards, providing a strong economic incentive to act honestly.

Fees on the Avalanche Blockchain

1. Transaction Fees:

- Dynamic Fees: Transaction fees on Avalanche are dynamic, varying based on network demand and the complexity of the transactions. This ensures that fees remain fair and proportional to the network's usage.
- Fee Burning: A portion of the transaction fees is burned, permanently removing them from circulation. This deflationary mechanism helps to balance the inflation from block rewards and incentivizes token holders by potentially increasing the value of AVAX over time.

2. Smart Contract Fees:

Execution Costs: Fees for deploying and interacting with smart contracts are determined by the computational resources required. These fees ensure that the network remains efficient and that resources are used responsibly.

3. Asset Creation Fees:

New Asset Creation: There are fees associated with creating new assets (tokens) on the Avalanche network. These fees help to prevent spam and ensure that only serious projects use the network's resources.

Base is a Layer-2 (L2) solution on Ethereum that uses optimistic rollups provided by the OP Stack on which it was developed. Transaction on base are bundled by a, so called, sequencer and the result is regularly submitted as an Layer-1 (L1) transactions. This way many L2 transactions get combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use base rather than the L1, i.e. Ethereum, itself.

To get crypto-assets in and out of base, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2 an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains unchallenged for a period of time the funds can be withdrawn. During this time period any other user can submit a fault proof, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour.

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.

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees.

Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity.

This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity.

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.

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, an Ethereum Layer 2 scaling solution, uses Optimistic Rollups to increase transaction throughput and reduce costs while maintaining security and decentralization.

Incentive Mechanisms:

1. Sequencers:

- Transaction Ordering: Sequencers are responsible for ordering and batching transactions off-chain. They play a critical role in maintaining the efficiency and speed of the network.
- Economic Incentives: Sequencers earn transaction fees from users. These fees incentivize sequencers to process transactions quickly and accurately.

2. Validators and Fraud Proofs:

- Assumption of Validity: In Optimistic Rollups, transactions are assumed to be valid by default. This allows for quick transaction finality.
- Challenge Mechanism: Validators (or anyone) can challenge the validity of a transaction by submitting a fraud proof during a specified challenge period. This mechanism ensures that invalid transactions are detected and reverted.
- Challenge Rewards: Successful challengers are rewarded for identifying and proving fraudulent transactions. This incentivizes participants to actively monitor the network for invalid transactions, thereby enhancing security.

3. Economic Penalties:

- **Fraud Proof Penalties:** If a sequencer includes an invalid transaction and it is successfully challenged, they face economic penalties, such as losing a portion of their staked collateral. This discourages dishonest behavior.
- **Inactivity and Misbehavior:** Validators and sequencers are also incentivized to remain active and behave correctly, as inactivity or misbehavior can lead to penalties and loss of rewards.

Fees Applicable on the Optimism Layer 2 Protocol:

1. Transaction Fees:

- **Layer 2 Transaction Fees:** Users pay fees for transactions processed on the Layer 2 network. These fees are generally lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
- **Cost Efficiency:** By batching multiple transactions into a single batch, Optimism reduces the overall cost per transaction, making it more economical for users.

2. L1 Data Fees:

- **Posting Batches to Ethereum:** Periodically, the state updates from Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee known as the L1 data fee, which covers the gas cost of publishing these state updates on Ethereum.
- **Cost Sharing:** The fixed costs of posting state updates to Ethereum are spread across multiple transactions within a batch, reducing the cost burden on individual transactions.

3. Smart Contract Fees:

- **Execution Costs:** Fees for deploying and interacting with smart contracts on Optimism are based on the computational resources required. This ensures that users are charged proportionally for the resources they consume.

Polygon uses a combination of Proof of Stake (PoS) and the Plasma framework to ensure network security, incentivize participation, and maintain transaction integrity.

Incentive Mechanisms:

1. Validators:

- **Staking Rewards:** Validators on Polygon secure the network by staking MATIC tokens. They are selected to validate transactions and produce new blocks based on the number of tokens they have staked. Validators earn rewards in the form of newly minted MATIC tokens and transaction fees for their services.
- **Block Production:** Validators are responsible for proposing and voting on new blocks. The selected validator proposes a block, and other validators verify and validate it. Validators are incentivized to act honestly and efficiently to earn rewards and avoid penalties.
- **Checkpointing:** Validators periodically submit checkpoints to the Ethereum main chain, ensuring the security and finality of transactions processed on Polygon. This provides an additional layer of security by leveraging Ethereum's robustness.

2. Delegators:

- **Delegation:** Token holders who do not wish to run a validator node can delegate their MATIC tokens to trusted validators. Delegators earn a portion of the rewards earned by the validators, incentivizing them to choose reliable and performant validators.
- **Shared Rewards:** Rewards earned by validators are shared with delegators, based on the proportion of tokens delegated. This system encourages widespread participation and enhances the network's decentralization.

3. Economic Security:

- **Slashing:** Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or

going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions.

- Bond Requirements: Validators are required to bond a significant amount of MATIC tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity. Fees on the Polygon Blockchain

4. Transaction Fees:

- Low Fees: One of Polygon's main advantages is its low transaction fees compared to the Ethereum main chain. The fees are paid in MATIC tokens and are designed to be affordable to encourage high transaction throughput and user adoption.
- Dynamic Fees: Fees on Polygon can vary depending on network congestion and transaction complexity. However, they remain significantly lower than those on Ethereum, making Polygon an attractive option for users and developers.

5. Smart Contract Fees:

Deployment and Execution Costs: Deploying and interacting with smart contracts on Polygon incurs fees based on the computational resources required. These fees are also paid in MATIC tokens and are much lower than on Ethereum, making it cost-effective for developers to build and maintain decentralized applications (dApps) on Polygon.

6. Plasma Framework:

State Transfers and Withdrawals: The Plasma framework allows for off-chain processing of transactions, which are periodically batched and committed to the Ethereum main chain. Fees associated with these processes are also paid in MATIC tokens, and they help reduce the overall cost of using the network.

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 SOL 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.

Solana'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.

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's consensus mechanism, the Stellar Consensus Protocol (SCP), is designed to achieve decentralized and secure transaction validation through a federated Byzantine agreement (FBA) model. Unlike Proof of Work (PoW) or Proof of Stake (PoS) systems, Stellar does not rely on direct economic incentives like mining rewards. Instead, it ensures network security and transaction validation through intrinsic network mechanisms and transaction fees.

Incentive Mechanisms:

1. Quorum Slices and Trust:

- Quorum Slices: Each node in the Stellar network selects other nodes it trusts to form a quorum slice. Consensus is achieved through the intersection of these slices, creating a robust and decentralized trust network.
- Federated Voting: Nodes communicate their votes within their quorum slices, and through multiple rounds of federated voting, they agree on the transaction state. This process ensures that even if some nodes are compromised, the network can still achieve consensus securely.

2. Intrinsic Value and Participation:

- Network Value: The intrinsic value of participating in a secure, efficient, and reliable payment network incentivizes nodes to act honestly and maintain network security. Organizations and individuals running nodes benefit from the network's functionality and the ability to facilitate transactions.
- Decentralization: By allowing nodes to choose their own quorum slices, Stellar promotes decentralization, reducing the risk of central points of failure and making the network more resilient to attacks. Fees on the Stellar Blockchain

3. Transaction Fees:

- Flat Fee Structure: Each transaction on the Stellar network incurs a flat fee of 0.00001 XLM (known as a base fee). This low and predictable fee structure makes Stellar suitable for micropayments and high-volume transactions.
- Spam Prevention: The transaction fee serves as a deterrent against spam attacks. By requiring a small fee for each transaction, Stellar ensures that the network remains efficient and that resources are not wasted on processing malicious or frivolous transactions.

4. Operational Costs:

Minimal Fees: The minimal transaction fees on Stellar not only prevent spam but also cover the operational costs of running the network. This ensures that the network can sustain itself without placing a significant financial burden on users.

5. Reserve Requirements:

- Account Reserves: To create a new account on the Stellar network, a minimum balance of 1 XLM is required. This reserve requirement prevents the creation of an excessive number of accounts, further protecting the network from spam and ensuring efficient resource usage.
- Trustline and Offer Reserves: Additional reserve requirements exist for creating trustlines and offers on the Stellar decentralized exchange (DEX). These reserves help maintain network integrity and prevent abuse.

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, linea, near_protocol, optimism, plume, polygon, ripple, sei, solana, sonic, 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.

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.

This report was provided by:

Crypto Risk Metrics

The IDW PS 951-certified SaaS tool “Crypto Risk Metrics” supports regulated financial institutions in the risk-based assessment of cryptocurrencies, Delta-1 Certificates (“Crypto ETPs”) and tokenized securities. ESG data, market conformity checks and KARBV-compliant price data complete the product range.

As a professional compliance expert, we provide support with:

**ESG data for
crypto-assets**

**White Papers for
crypto-assets**

**Risk
management**

**Compliant
price data**

**Market
conformity check**