dwpbank

Sustainability indicators for crypto-assets

Disclosures pursuant to Article 66(5) MiCA

This report was provided by:

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

2026-08-13

Table of Contents

Preamble

About the Crypto-Asset Service Provider (CASP)

Name of the CASP: Deutsche WertpapierService Bank AG
Street and number: Wildunger Straße 14
City: Frankfurt am Main
Country: Germany
LEI: 529900EXG2PM316ISO63

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	150,057,306,648.79
2	Ethereum Eth	D5RG2FHH0	2,159,953.20
3	Polygon POL	GB8DQ8DWN	96,475.21
4	Uniswap	XMB84LZBZ	6,367.03
5	ChainLink Token	3R3J70FDR	4,962.82
6	Aave Token	H618RN577	2,452.96

Sustainability indicators

Bitcoin

BTC | V15WLZJMF

Quantitative information

Quantitative sustainability indicators for Bitcoin

Field	Value	Unit
S.1 Name	Deutsche WertpapierService Bank AG	/
S.2 Relevant legal entity identifier	529900EXG2PM316ISO63	/
S.3 Name of the crypto-asset	Bitcoin	/
S.6 Beginning of the period to which the disclosure relates	2025-08-13	/
S.7 End of the period to which the disclosure relates	2026-08-13	/
S.8 Energy consumption	150057306648.78644	kWh/a
S.10 Renewable energy consumption	34.4781471084	%
S.11 Energy intensity	6.71559	kWh
S.12 Scope 1 DLT GHG emissions – Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emissions – Purchased	61823019.31322	tCO2e
S.14 GHG intensity	2.76680	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.

Ethereum Eth

ETH | D5RG2FHH0

Quantitative information

Quantitative sustainability indicators for Ethereum Eth

Field	Value	Unit
S.1 Name	Deutsche WertpapierService Bank AG	/
S.2 Relevant legal entity identifier	529900EXG2PM316ISO63	/
S.3 Name of the crypto-asset	Ethereum Eth	/
S.6 Beginning of the period to which the disclosure relates	2025-08-13	/
S.7 End of the period to which the disclosure relates	2026-08-13	/
S.8 Energy consumption	2159953.20000	kWh/a
S.10 Renewable energy consumption	37.9124101186	%
S.11 Energy intensity	0.00004	kWh
S.12 Scope 1 DLT GHG emissions – Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emissions – Purchased	718.86066	tCO2e
S.14 GHG intensity	0.00001	kgCO2e

Qualitative information

S.4 Consensus Mechanism

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.

S.5 Incentive Mechanisms and Applicable Fees

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.

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. 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.

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.

Polygon POL

MATIC | GB8DQ8DWN

Quantitative information

Quantitative sustainability indicators for Polygon POL

Field	Value	Unit
S.1 Name	Deutsche WertpapierService Bank AG	/
S.2 Relevant legal entity identifier	529900EXG2PM316ISO63	/
S.3 Name of the crypto-asset	Polygon POL	/
S.6 Beginning of the period to which the disclosure relates	2025-08-13	/
S.7 End of the period to which the disclosure relates	2026-08-13	/
S.8 Energy consumption	96475.20781	kWh/a

Qualitative information

S.4 Consensus Mechanism

Polygon POL is present on the following networks: Ethereum, Polygon.

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

Polygon POL is present on the following networks: Ethereum, Polygon.

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:

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, ethereum, 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.

To determine the energy consumption of a token, the energy consumption of the network(s) ethereum 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.

Uniswap

UNI | XMB84LZBZ

Quantitative information

Quantitative sustainability indicators for Uniswap

Field	Value	Unit
S.1 Name	Deutsche WertpapierService Bank AG	/
S.2 Relevant legal entity identifier	529900EXG2PM316ISO63	/
S.3 Name of the crypto-asset	Uniswap	/
S.6 Beginning of the period to which the disclosure relates	2025-08-13	/
S.7 End of the period to which the disclosure relates	2026-08-13	/
S.8 Energy consumption	6367.02997	kWh/a

Qualitative information

S.4 Consensus Mechanism

Uniswap is present on the following networks: Arbitrum, Binance Smart Chain, Ethereum, Polygon.

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.

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof-of-Staked-Authority (PoSA), which combines elements of Delegated-Proof-of-Stake (DPoS) and Proof-of-Authority (PoA). This method is intended to support fast block times and low fees while maintaining a level of decentralisation and security. Validators are responsible for producing blocks, validating transactions, and maintaining network security. The validator set consists of up to 45 validators, including 21 “Cabinet” validators and 24 “Candidate” validators, selected based on bonded stake. A subset of validators is selected per epoch to participate in block production. Token holders may delegate BNB to validators to support their selection. Delegators share in the rewards generated by validators, providing an economic incentive to participate in staking. Validator candidates are nodes

that have staked BNB but are not part of the primary validator subset for a given epoch. They may be selected into the active set based on staking rank and can participate in block production with lower probability. Validators are ranked based on the amount of bonded BNB and are updated periodically. Validators must stake BNB as collateral and may be subject to slashing in cases of misbehaviour, including double-signing, malicious voting, or prolonged downtime.

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

Uniswap is present on the following networks: Arbitrum, Binance Smart Chain, Ethereum, Polygon.

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.

Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure. BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission. BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information. Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance. Transaction fees on BSC are paid in BNB and are intended to compensate validators for maintaining the network. BSC is designed as a comparatively low-fee network, and smart-contract transactions and transfers require gas fees in BNB. BSC does not rely on a separate protocol-level block reward. Instead, staking rewards are derived from transaction fees. Most of the block fee is allocated to the proposing validator, then split between validator commission and delegator-linked reward distribution. Part of transaction-fee revenue is collected through the System Reward Contract and used for designated system purposes, including fast-finality rewards. Deploying and interacting with smart contracts on BSC requires payment of gas fees in BNB. These fees depend on the computational resources required and form part of the network's overall fee and validator-incentive model.

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) arbitrum, binance_smart_chain, 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.

ChainLink Token

LINK | 3R3J70FDR

Quantitative information

Quantitative sustainability indicators for ChainLink Token

Field	Value	Unit
S.1 Name	Deutsche WertpapierService Bank AG	/
S.2 Relevant legal entity identifier	529900EXG2PM316ISO63	/
S.3 Name of the crypto-asset	ChainLink Token	/
S.6 Beginning of the period to which the disclosure relates	2025-08-13	/
S.7 End of the period to which the disclosure relates	2026-08-13	/
S.8 Energy consumption	4962.82463	kWh/a

Qualitative information

S.4 Consensus Mechanism

ChainLink Token is present on the following networks: Arbitrum, Avalanche, Binance Smart Chain, Ethereum, Fantom, Gnosis Chain, Optimism, Polygon, Solana.

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.

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof-of-Staked-Authority (PoSA), which combines elements of Delegated-Proof-of-Stake (DPoS) and Proof-of-Authority (PoA). This method is intended to support fast block times and low fees while maintaining a level of decentralisation and security. Validators are responsible for producing blocks, validating transactions, and maintaining network security. The validator set consists of up to 45 validators, including 21 “Cabinet” validators and 24 “Candidate” validators, selected based on bonded stake. A subset of validators is selected per epoch to participate in block production. Token holders may delegate BNB to validators to support their selection. Delegators share in the rewards generated by validators, providing an economic incentive to participate in staking. Validator candidates are nodes that have staked BNB but are not part of the primary validator subset for a given epoch. They may be selected into the active set based on staking rank and can participate in block production with lower probability. Validators are ranked based on the amount of bonded BNB and are updated periodically. Validators must stake BNB as collateral and may be subject to slashing in cases of misbehaviour, including double-signing, malicious voting, or prolonged downtime.

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.

Fantom operates on the Lachesis Protocol, an Asynchronous Byzantine Fault Tolerant (aBFT) consensus mechanism designed for fast, secure, and scalable transactions.

Core Components of Fantom’s Consensus:

1. Lachesis Protocol (aBFT):
   - Asynchronous and Leaderless: Lachesis allows nodes to reach consensus independently without relying on a central leader, enhancing decentralization and speed.
   - DAG Structure: Instead of a linear blockchain, Lachesis uses a Directed Acyclic Graph (DAG) structure, allowing multiple transactions to be processed in parallel across nodes. This structure supports high throughput, making the network suitable for applications requiring rapid transaction processing.

2. Event Blocks and Instant Finality:
   - Event Blocks: Transactions are grouped into event blocks, which are validated asynchronously by multiple validators. When enough validators confirm an event block, it becomes part of the Fantom network's history.
   - Instant Finality: Transactions on Fantom achieve immediate finality, meaning they are confirmed and cannot be reversed. This property is ideal for applications requiring fast and irreversible transactions.

Gnosis Chain – Consensus Mechanism Gnosis Chain employs a dual-layer structure to balance scalability and security, using Proof of Stake (PoS) for its core consensus and transaction finality.

Core Components:

- Two-Layer Structure Layer 1: Gnosis Beacon Chain The Gnosis Beacon Chain operates on a Proof of Stake (PoS) mechanism, acting as the security and consensus backbone. Validators stake GNO tokens on the Beacon Chain and validate transactions, ensuring network security and finality.
- Layer 2: Gnosis xDai Chain processes transactions and dApp interactions, providing high-speed, low-cost transactions. Layer 2 transaction data is finalized on the Gnosis Beacon Chain, creating an integrated framework where Layer 1 ensures security and finality, and Layer 2 enhances scalability. Validator Role and Staking Validators on the Gnosis Beacon Chain stake GNO tokens and participate in consensus by validating blocks. This setup ensures that validators have an economic interest in maintaining the security and integrity of both the Beacon Chain (Layer 1) and the xDai Chain (Layer 2). Cross-Layer Security Transactions on Layer 2 are ultimately finalized on Layer 1, providing security and finality to all activities on the Gnosis Chain. This architecture allows Gnosis Chain to combine the speed and cost efficiency of Layer 2 with the security guarantees of a PoS-secured Layer 1, making it suitable for both high-frequency applications and secure asset management.

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.

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.

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.

S.5 Incentive Mechanisms and Applicable Fees

ChainLink Token is present on the following networks: Arbitrum, Avalanche, Binance Smart Chain, Ethereum, Fantom, Gnosis Chain, Optimism, Polygon, Solana.

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.

Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure. BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission. BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information. Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance. Transaction fees on BSC are paid in BNB and are intended to compensate validators for maintaining the network. BSC is designed as a comparatively low-fee network, and smart-contract transactions and transfers require gas fees in BNB. BSC does not rely on a separate protocol-level block reward. Instead, staking rewards are derived from transaction fees. Most of the block fee is allocated to the proposing validator, then split between validator commission and delegator-linked reward distribution. Part of transaction-fee revenue is collected through the System Reward Contract and used for designated system purposes, including fast-finality rewards. Deploying and interacting with smart contracts on BSC requires payment of gas fees in BNB. These fees depend on the computational resources required and form part of the network's overall fee and validator-incentive model.

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.

Fantom's incentive model promotes network security through staking rewards, transaction fees, and delegation options, encouraging broad participation.

Incentive Mechanisms:

1. Staking Rewards for Validators:
   - Earning Rewards in FTM: Validators who participate in the consensus process earn rewards in FTM tokens, proportional to the amount they have staked. This incentivizes validators to actively secure the network.

- Dynamic Staking Rate: Fantom's staking reward rate is dynamic, adjusting based on total FTM staked across the network. As more FTM is staked, individual rewards may decrease, maintaining a balanced reward structure that supports long-term network security.

2. Delegation for Token Holders:
   Delegated Staking: Users who do not operate validator nodes can delegate their FTM tokens to validators. In return, they share in the staking rewards, encouraging wider participation in securing the network.

Applicable Fees:

- Transaction Fees in FTM: Users pay transaction fees in FTM tokens. The network's high throughput and DAG structure keep fees low, making Fantom ideal for decentralized applications (dApps) requiring frequent transactions.
- Efficient Fee Model: The low fees and scalability of the network make it cost-effective for users, fostering a favorable environment for high-volume applications.

The Gnosis Chain's incentive and fee models encourage both validator participation and network accessibility, using a dual-token system to maintain low transaction costs and effective staking rewards.

Incentive Mechanisms:

- Staking Rewards for Validators GNO Rewards: Validators earn staking rewards in GNO tokens for their participation in consensus and securing the network.
- Delegation Model: GNO holders who do not operate validator nodes can delegate their GNO tokens to validators, allowing them to share in staking rewards and encouraging broader participation in network security.
- Dual-Token Model GNO: Used for staking, governance, and validator rewards, GNO aligns long-term network security incentives with token holders' economic interests.
- xDai: Serves as the primary transaction currency, providing stable and low-cost transactions. The use of a stable token (xDai) for fees minimizes volatility and offers predictable costs for users and developers.

Applicable Fees:

Transaction Fees in xDai Users pay transaction fees in xDai, the stable fee token, making costs affordable and predictable. This model is especially suited for high-frequency applications and dApps where low transaction fees are essential. xDai transaction fees are redistributed to validators as part of their compensation, aligning their rewards with network activity. Delegated Staking Rewards Through delegated staking, GNO holders can earn a share of staking rewards by delegating their tokens to active validators, promoting user participation in network security without requiring direct involvement in consensus operations.

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.

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.

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.

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) arbitrum, avalanche, binance_smart_chain, ethereum, fantom, gnosis_chain, optimism, polygon, solana 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.

Aave Token

AAVE | H618RN577

Quantitative information

Quantitative sustainability indicators for Aave Token

Field	Value	Unit
S.1 Name	Deutsche WertpapierService Bank AG	/
S.2 Relevant legal entity identifier	529900EXG2PM316ISO63	/
S.3 Name of the crypto-asset	Aave Token	/
S.6 Beginning of the period to which the disclosure relates	2025-08-13	/
S.7 End of the period to which the disclosure relates	2026-08-13	/
S.8 Energy consumption	2452.96402	kWh/a

Qualitative information

S.4 Consensus Mechanism

Aave Token is present on the following networks: Avalanche, Binance Smart Chain, Ethereum, Gnosis Chain, Huobi, Near Protocol, Polygon, Solana.

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.

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof-of-Staked-Authority (PoSA), which combines elements of Delegated-Proof-of-Stake (DPoS) and Proof-of-Authority (PoA). This method is intended to support fast block times and low fees while maintaining a level of decentralisation and security. Validators are responsible for producing blocks, validating transactions, and maintaining network security. The validator set consists of up to 45 validators, including 21 “Cabinet” validators and 24 “Candidate” validators, selected based on bonded stake. A subset of validators is selected per epoch to participate in block production. Token holders may delegate BNB to validators to support their selection. Delegators share in the rewards generated by validators, providing an economic incentive to participate in staking. Validator candidates are nodes that have staked BNB but are not part of the primary validator subset for a given epoch. They may be selected into the active set based on staking rank and can participate in block production with lower probability. Validators are ranked based on the amount of bonded BNB and are updated periodically. Validators must stake BNB as collateral and may be subject to slashing in cases of misbehaviour, including double-signing, malicious voting, or prolonged downtime.

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.

Gnosis Chain – Consensus Mechanism Gnosis Chain employs a dual-layer structure to balance scalability and security, using Proof of Stake (PoS) for its core consensus and transaction finality.

Core Components:

- Two-Layer Structure Layer 1: Gnosis Beacon Chain The Gnosis Beacon Chain operates on a Proof of Stake (PoS) mechanism, acting as the security and consensus backbone. Validators stake GNO tokens on the Beacon Chain and validate transactions, ensuring network security and finality.
- Layer 2: Gnosis xDai Chain processes transactions and dApp interactions, providing high-speed, low-cost transactions. Layer 2 transaction data is finalized on the Gnosis Beacon Chain, creating an integrated framework where Layer 1 ensures security and finality, and Layer 2 enhances scalability. Validator Role and Staking Validators on the Gnosis Beacon Chain stake GNO tokens and participate in consensus by validating blocks. This setup ensures that validators have an economic interest in maintaining the security and integrity of both the Beacon Chain (Layer 1) and the xDai Chain (Layer 2). Cross-Layer Security Transactions on Layer 2 are ultimately finalized on Layer 1, providing security and finality to all activities on the Gnosis Chain. This architecture allows Gnosis Chain to combine the speed and cost efficiency of Layer 2 with the security guarantees of a PoS-secured Layer 1, making it suitable for both high-frequency applications and secure asset management.

The Huobi Eco Chain (HECO) blockchain employs a Hybrid-Proof-of-Stake (HPoS) consensus mechanism, combining elements of Proof-of-Stake (PoS) to enhance transaction efficiency and scalability.

Key Features of HECO's Consensus Mechanism:

1. Validator Selection: HECO supports up to 21 validators, selected based on their stake in the network.
2. Transaction Processing: Validators are responsible for processing transactions and adding blocks to the blockchain.
3. Transaction Finality: The consensus mechanism ensures quick finality, allowing for rapid confirmation of transactions.
4. Energy Efficiency: By utilizing PoS elements, HECO reduces energy consumption compared to traditional Proof-of-Work systems.

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.

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.

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.

S.5 Incentive Mechanisms and Applicable Fees

Aave Token is present on the following networks: Avalanche, Binance Smart Chain, Ethereum, Gnosis Chain, Huobi, Near Protocol, Polygon, Solana.

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.

Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure. BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission. BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information. Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance. Transaction fees on BSC are paid in BNB and are intended to compensate validators for maintaining the network. BSC is designed as a comparatively low-fee network, and smart-contract transactions and transfers require gas fees in BNB. BSC does not rely on a separate protocol-level block reward. Instead, staking rewards are derived from transaction fees. Most of the block fee is allocated to the proposing validator, then split between validator commission and delegator-linked reward distribution. Part of transaction-fee revenue is collected through the System Reward Contract and used for designated system purposes, including fast-finality rewards. Deploying and interacting with smart contracts on BSC requires payment of gas fees in BNB. These fees depend on the computational resources required and form part of the network's overall fee and validator-incentive model.

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.

The Gnosis Chain's incentive and fee models encourage both validator participation and network accessibility, using a dual-token system to maintain low transaction costs and effective staking rewards.

Incentive Mechanisms:

- Staking Rewards for Validators GNO Rewards: Validators earn staking rewards in GNO tokens for their participation in consensus and securing the network.

- Delegation Model: GNO holders who do not operate validator nodes can delegate their GNO tokens to validators, allowing them to share in staking rewards and encouraging broader participation in network security.
- Dual-Token Model GNO: Used for staking, governance, and validator rewards, GNO aligns long-term network security incentives with token holders' economic interests.
- xDai: Serves as the primary transaction currency, providing stable and low-cost transactions. The use of a stable token (xDai) for fees minimizes volatility and offers predictable costs for users and developers.

Applicable Fees:

Transaction Fees in xDai Users pay transaction fees in xDai, the stable fee token, making costs affordable and predictable. This model is especially suited for high-frequency applications and dApps where low transaction fees are essential. xDai transaction fees are redistributed to validators as part of their compensation, aligning their rewards with network activity. Delegated Staking Rewards Through delegated staking, GNO holders can earn a share of staking rewards by delegating their tokens to active validators, promoting user participation in network security without requiring direct involvement in consensus operations.

The Huobi Eco Chain (HECO) blockchain employs a Hybrid-Proof-of-Stake (HPoS) consensus mechanism, combining elements of Proof-of-Stake (PoS) to enhance transaction efficiency and scalability.

Incentive Mechanism:

1. Validator Rewards:
   Validators are selected based on their stake in the network. They process transactions and add blocks to the blockchain. Validators receive rewards in the form of transaction fees for their role in maintaining the blockchain's integrity.
2. Staking Participation:
   Users can stake Huobi Token (HT) to become validators or delegate their tokens to existing validators. Staking helps secure the network and, in return, participants receive a portion of the transaction fees as rewards.

Applicable Fees:

1. Transaction Fees (Gas Fees):
   Users pay gas fees in HT tokens to execute transactions and interact with smart contracts on the HECO network. These fees compensate validators for processing and validating transactions.
2. Smart Contract Execution Fees:
   Deploying and interacting with smart contracts incur additional fees, which are also paid in HT tokens. These fees cover the computational resources required to execute contract code.

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.

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.

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.

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) avalanche, binance_smart_chain, ethereum, gnosis_chain, huobi, near_protocol, polygon, solana 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