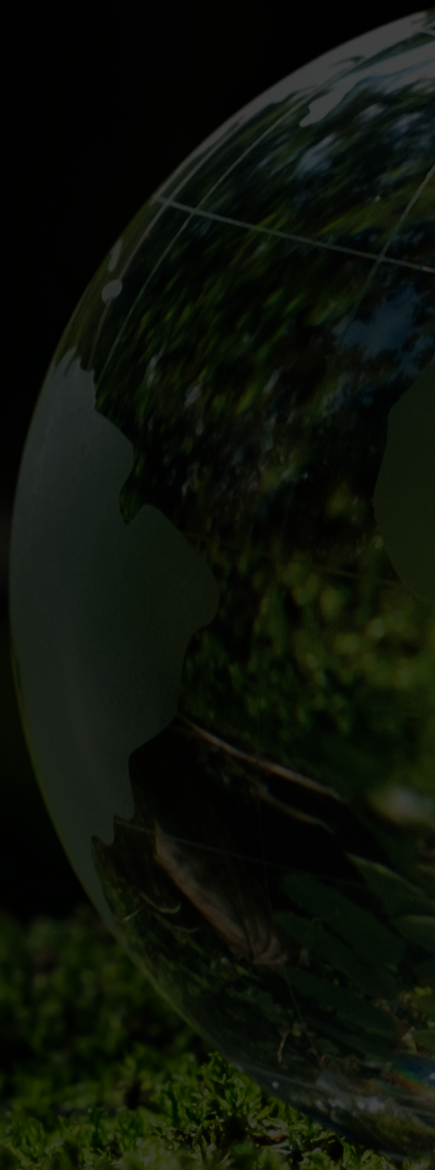
Bank Frick

Sustainability indicators for crypto-assets

Disclosures in accordance with Article 66 (5) MiCAR.



This report was provided by Crypto Risk Metrics.

2025-07-01

Table of Content

Preamble

About Crypto Asset Service Provider (CASP)

Name of the CASP: Bank Frick AG
Street and number: Landstrasse 14
City: Balzers
Country: Liechtenstein
LEI: 529900RQOBT3ZJMDRK43

About this report

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

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

Overview

This is an overview of the core indicator energy consumption but does not represent the reporting according to MiCAR 66 (5). Please find the full disclosure below.

#	Crypto-Asset Name	Crypto-Asset FFG	Energy consumption (kWh per calendar year)
1	Bitcoin	V15WLZJMF	182,841,389,361.36
2	Litecoin	D74JZ1VRD	1,168,654,780.56
3	Bitcoin Cash	919BF3W7L	978,793,416.99
4	Solana SOL	6QZ1LNC12	6,244,785.00
5	Ethereum Eth	D5RG2FHH0	2,207,257.20
6	NEAR Protocol	MXXM59Z0T	919,965.15
7	Avalanche AVAX	S6JCBF70N	819,810.70
8	Cardano ADA	76QS7QCXB	813,103.20
9	Polkadot DOT	SGD9NLTRG	630,739.35
10	USDC	TJWK5QTRK	462,659.31
11	Tezos	FLJPFR9RS	282,247.67
12	Cosmos ATOM	6C7F2WVZH	186,472.75
13	Polygon POL	GB8DQ8DWN	92,462.13
14	Stellar Lumen	ZCN8SR2H7	52,560.00
15	ChainLink Token	3R3J70FDR	5,018.30

Sustainability indicators

Bitcoin

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Bitcoin	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	182841389361.36044	kWh/a
S.10 Renewable energy consumption	24.1347029759	%
S.11 Energy intensity	12.32300	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	75329932.26515	tCO2e
S.14 GHG intensity	5.07703	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.

Litecoin

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Litecoin	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	1168654780.55749	kWh/a
S.10 Renewable energy consumption	24.1347029759	%
S.11 Energy intensity	0.04664	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	481481.16665	tCO2e
S.14 GHG intensity	0.01921	kgCO2e

Qualitative information

S.4 Consensus Mechanism

Litecoin, like Bitcoin, uses Proof of Work (PoW) as its consensus mechanism, but with a few key differences:

1. Scrypt Hashing Algorithm: Unlike Bitcoin’s SHA-256 algorithm, Litecoin uses the Scrypt hashing algorithm, which is more memory-intensive. This makes mining Litecoin more accessible to regular users and limits the advantages of specialized hardware (like ASICs) in the early years.
2. Mining and Block Creation: Miners compete to solve cryptographic puzzles and, upon success, add new blocks to the blockchain. This process involves solving the Scrypt algorithm, which requires computational work. The first miner to solve the problem earns the block reward and transaction fees associated with the transactions in the block.
3. Block Time: Litecoin has a block time of 2.5 minutes, much faster than Bitcoin’s 10 minutes. This means transactions confirm more quickly, increasing the overall network speed.
4. Block Reward Halving: Similar to Bitcoin, Litecoin has a block reward halving event approximately every four years. Initially, miners earned 50 LTC per block, but this reward decreases by half after each halving event. This process continues until the maximum supply of 84 million LTC is reached.

5. Difficulty Adjustment: Litecoin adjusts the mining difficulty approximately every 2,016 blocks (about every 3.5 days) to ensure that blocks continue to be mined at a consistent rate of 2.5 minutes per block, regardless of fluctuations in the total network hash rate.

S.5 Incentive Mechanisms and Applicable Fees

Litecoin, like Bitcoin, uses the Proof of Work (PoW) consensus mechanism to secure transactions and incentivize miners.

Incentive Mechanisms:

1. Mining Rewards:
   Block Rewards: Miners are rewarded with Litecoin (LTC) for successfully mining new blocks. Initially, miners received 50 LTC per block, but this reward halves approximately every four years. Transaction Fees: Miners also earn transaction fees from the transactions included in the blocks they mine. Users pay fees to have their transactions processed by miners, especially when they need faster confirmation times.
2. Halving:
   The halving mechanism ensures that over time, fewer Litecoins are introduced into circulation, creating a deflationary model. This makes mining more valuable as the circulating supply becomes scarcer, incentivizing miners to continue participating in the network even as block rewards decrease.
3. Economic Security:
   The cost of mining (e.g., hardware and electricity) provides a strong economic incentive for miners to act honestly. If miners attempt to cheat or attack the network, they risk losing the computational work they invested, as invalid blocks will be rejected by the network.

Fees on the Litecoin Blockchain:

- Transaction Fees: Litecoin users pay a transaction fee for each transaction, typically calculated in LTC per byte of transaction data. The fees are dynamic and vary based on network congestion.
- Low Fees: Litecoin is known for its relatively low transaction fees compared to other blockchains like Bitcoin, which makes it ideal for smaller transactions and micro-payments.
- Fee Redistribution: Collected transaction fees are distributed to miners as part of their rewards for validating transactions and securing the network.

S.9 Energy consumption sources and methodologies

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: Scrypt. 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.

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.

Bitcoin Cash

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Bitcoin Cash	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	978793416.98728	kWh/a
S.10 Renewable energy consumption	24.1347029759	%
S.11 Energy intensity	0.05209	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e

Field	Value	Unit
S.13 Scope 2 DLT GHG emission - Purchased	403259.03266	tCO2e
S.14 GHG intensity	0.02146	kgCO2e

Qualitative information

S.4 Consensus Mechanism

Bitcoin Cash is present on the following networks: Bitcoin Cash, Smart Bitcoin Cash.

The Bitcoin Cash blockchain network uses a consensus mechanism called Proof of Work (PoW) to achieve distributed consensus among its nodes. It originated from the Bitcoin blockchain, hence has the same consensus mechanisms but with a larger block size, which makes it more centralized.

Core Concepts:

1. Nodes and Miners:
   - Nodes: Nodes are computers running the Bitcoin Cash 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 Cash 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 Cash 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.

Smart Bitcoin Cash (SmartBCH) operates as a sidechain to Bitcoin Cash (BCH), leveraging a hybrid consensus mechanism combining Proof of Work (PoW) compatibility and validator-based validation.

Core Components:
- Proof of Work Compatibility: SmartBCH relies on Bitcoin Cash's PoW for settlement and security, ensuring robust integration with BCH's main chain. SHA-256 Algorithm: Uses the same SHA-256 hashing algorithm as Bitcoin Cash, allowing compatibility with existing mining hardware and infrastructure.
- Consensus via Validators: Transactions within SmartBCH are validated by a set of validators chosen based on staking and operational efficiency. This hybrid approach combines the hash power of PoW with a validator-based model to enhance scalability and flexibility.

S.5 Incentive Mechanisms and Applicable Fees

Bitcoin Cash is present on the following networks: Bitcoin Cash, Smart Bitcoin Cash.

The Bitcoin Cash blockchain operates on a Proof-of-Work (PoW) consensus mechanism, with incentives and fee structures designed to support miners and the overall network's sustainability:

Incentive Mechanism:

1. Block Rewards:
   - Newly Minted Bitcoins: Miners receive a block reward, which consists of newly created bitcoins for successfully mining a new block. Initially, the reward was 50 BCH, but it halves approximately every four years in an event known as the "halving."
   - Halving and Scarcity: The halving ensures that the total supply of Bitcoin Cash is capped at 21 million BCH, creating scarcity that could drive up value over time.
2. Transaction Fees:
   - User Fees: Each transaction includes a fee, paid by users, that incentivizes miners to include the transaction in a new block. This fee market becomes increasingly important as block rewards decrease over time due to the halving events.
   - Fee Market: Transaction fees are market-driven, with users competing to get their transactions included quickly. Higher fees lead to faster transaction processing, especially during periods of high network congestion.

Applicable Fees:

1. Transaction Fees:
   Bitcoin Cash transactions require a small fee, paid in BCH, which is determined by the transaction's size and the network demand at the time. These fees are crucial for the continued operation of the network, particularly as block rewards decrease over time due to halvings.
2. Fee Structure During High Demand:
   In times of high congestion, users may choose to increase their transaction fees to prioritize their transactions for faster processing. The fee structure ensures that miners are incentivized to prioritize higher-fee transactions.

SmartBCH's incentive model encourages validators and network participants to secure the sidechain and process transactions efficiently.

Incentive Mechanisms:

- Validator Rewards: Validators are rewarded with a share of transaction fees for their role in validating transactions and maintaining the network.

- Economic Alignment: The system incentivizes validators to act in the network's best interest, ensuring stability and fostering adoption through economic alignment.

Applicable Fees:

Transaction Fees: Fees for transactions on SmartBCH are paid in BCH, ensuring seamless integration with the Bitcoin Cash ecosystem.

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.

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.

Solana SOL

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Solana SOL	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	6244785.00000	kWh/a
S.10 Renewable energy consumption	27.0081797971	%
S.11 Energy intensity	0.00000	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	2116.16462	tCO2e
S.14 GHG intensity	0.00000	kgCO2e

Qualitative information

S.4 Consensus Mechanism

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

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

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.

Ethereum Eth

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Ethereum Eth	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	2207257.20000	kWh/a
S.10 Renewable energy consumption	26.5386870830	%
S.11 Energy intensity	0.00010	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	734.60405	tCO2e
S.14 GHG intensity	0.00003	kgCO2e

Qualitative information

S.4 Consensus Mechanism

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

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

S.5 Incentive Mechanisms and Applicable Fees

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

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

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

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.

NEAR Protocol

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	NEAR Protocol	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	919965.14766	kWh/a
S.10 Renewable energy consumption	26.1931959128	%
S.11 Energy intensity	0.00008	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	309.80486	tCO2e
S.14 GHG intensity	0.00003	kgCO2e

Qualitative information

S.4 Consensus Mechanism

NEAR Protocol is present on the following networks: Binance Smart Chain, Ethereum, Near Protocol.

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 ensures fast block times and low fees while maintaining a level of decentralization and security.

Core Components:

1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.
2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security.
3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process
4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes.

5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network.
6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives
7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB.
8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance.
9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

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

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

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.

S.5 Incentive Mechanisms and Applicable Fees

NEAR Protocol is present on the following networks: Binance Smart Chain, Ethereum, Near Protocol.

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators.

Incentive Mechanisms

1. Validators:
   - Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards.
   - Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks.
2. Delegators:
   - Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks.
   - Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network's security and decentralization by choosing reliable validators.
3. Candidates:
   Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience.
4. Economic Security:
   - Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network.
   - Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets.

Fees on the Binance Smart Chain

1. Transaction Fees:
   - Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators.

  - Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.
2. Block Rewards:
   Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions.
3. Cross-Chain Fees:
   Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience.
4. Smart Contract Fees:
   Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

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

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

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

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.

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. 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) binance_smart_chain, 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.

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.

Avalanche AVAX

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Avalanche AVAX	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	819810.70264	kWh/a
S.10 Renewable energy consumption	25.4207037379	%
S.11 Energy intensity	0.00007	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	307.81088	tCO2e
S.14 GHG intensity	0.00003	kgCO2e

Qualitative information

S.4 Consensus Mechanism

Avalanche AVAX is present on the following networks: Avalanche, Avalanche X Chain.

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

Avalanche Consensus Process:

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

The Avalanche X-Chain uses the Avalanche consensus protocol, which relies on repeated subsampling of validators to reach agreement on transactions.

S.5 Incentive Mechanisms and Applicable Fees

Avalanche AVAX is present on the following networks: Avalanche, Avalanche X Chain.

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

1. Validators:

Staking: Validators on the Avalanche network are required to stake AVAX tokens. The amount staked influences their probability of being selected to propose or validate new blocks.
Rewards: Validators earn rewards for their participation in the consensus process. These rewards are proportional to the amount of AVAX staked and their uptime and performance in validating transactions.

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

2. Economic Incentives:

Block Rewards: Validators receive block rewards for proposing and validating blocks. These rewards are distributed from the network's inflationary issuance of AVAX tokens.
Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This includes fees for simple transactions, smart contract interactions, and the creation of new assets on the network.

3. Penalties:

- Slashing: Unlike some other PoS systems, Avalanche does not employ slashing (i.e., the confiscation of staked tokens) as a penalty for misbehavior.Instead, the network relies on the financial disincentive of lost future rewards for validators who are not consistently online or act maliciously.
- Uptime Requirements: Validators must maintain a high level of uptime and correctly validate transactions to continue earning rewards. Poor performance or malicious actions result in missed rewards, providing a strong economic incentive to act honestly.

Fees on the Avalanche Blockchain

1. Transaction Fees:
   - Dynamic Fees: Transaction fees on Avalanche are dynamic, varying based on network demand and the complexity of the transactions. This ensures that fees remain fair and proportional to the network's usage.
   - Fee Burning: A portion of the transaction fees is burned, permanently removing them from circulation. This deflationary mechanism helps to balance the inflation from block rewards and incentivizes token holders by potentially increasing the value of AVAX over time.
2. Smart Contract Fees:
   Execution Costs: Fees for deploying and interacting with smart contracts are determined by the computational resources required. These fees ensure that the network remains efficient and that resources are used responsibly.
3. Asset Creation Fees:
   New Asset Creation: There are fees associated with creating new assets (tokens) on the Avalanche network. These fees help to prevent spam and ensure that only serious projects use the network's resources.

Validator incentives on the X-Chain are indirect and come from network-wide AVAX issuance. Transaction fees are fixed and burned to prevent spam and reduce the total supply of AVAX over time

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. 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) avalanche, avalanche_x_chain 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.

Cardano ADA

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Cardano ADA	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	813103.20000	kWh/a
S.10 Renewable energy consumption	26.1931305023	%
S.11 Energy intensity	0.00027	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	273.81815	tCO2e
S.14 GHG intensity	0.00009	kgCO2e

Qualitative information

S.4 Consensus Mechanism

Core Components: Cardano uses the Ouroboros consensus mechanism, a Proof of Stake (PoS) protocol designed for scalability, security, and energy efficiency.

Core Concepts:

1. Proof of Stake (PoS): Validators (called slot leaders) are selected based on the amount of ADA they have staked, rather than solving complex computational puzzles. Validators propose and validate blocks, which are added to the blockchain.
2. Epochs and Slot Leaders: Cardano divides time into epochs (fixed time periods), each of which is subdivided into slots. Slot leaders are selected for each slot to validate and propose blocks. Slot leaders are chosen randomly based on the amount of ADA staked. More stake increases the probability of being selected. Validators are responsible for confirming transactions during their slot and passing the block to the next slot leader.
3. Delegation and Staking Pools: ADA holders can delegate their tokens to staking pools, which increases the pool's chances of being selected to validate a block. The pool operator and delegators share the rewards based on their stakes. This system ensures that participants who do not want to operate a full validator node can still earn rewards and contribute to network security by supporting trusted staking pools.
4. Security and Adversary Resistance: Ouroboros ensures security even in the presence of potential attacks. It assumes that adversaries may attempt to propagate alternative chains or send arbitrary messages. The protocol is secure as long as more than 51% of the staked ADA is controlled by honest participants. Settlement Delay: To protect against adversarial attacks, the new slot leader must consider the last few blocks as transient. Only the blocks preceding these are treated as finalized, ensuring that chain finality is secure against manipulation attempts. This mechanism also allows participants to temporarily go offline and resynchronize as long as they are not disconnected for more than the settlement delay period.
5. Chain Selection: Cardano's nodes adopt the longest valid chain rule: each node stores a local copy of the blockchain and replaces it with any discovered valid, longer chain. This ensures that all nodes eventually converge on a single version of the blockchain, maintaining network consistency.

S.5 Incentive Mechanisms and Applicable Fees

Cardano uses incentive mechanisms to ensure network security and decentralization through staking rewards, slashing mechanisms, and transaction fees.

Incentive Mechanisms to Secure Transactions:

1. Staking Rewards:
   - Validators, known as slot leaders, secure the network by validating transactions and creating new blocks. To participate, validators must stake ADA, and those with larger stakes are more likely to be selected as slot leaders.
   - Validators are rewarded with newly minted ADA and transaction fees for successfully producing blocks and validating transactions.
   - Delegators, who may not wish to run a validator node, can delegate their ADA to staking pools. By doing so, they contribute to the network's security and earn a share of the rewards earned by the pool. The rewards are distributed proportionally based on the amount of ADA delegated.
2. Slashing Mechanism:
   - To prevent malicious behavior, Cardano employs a slashing mechanism. Validators who act dishonestly, fail to validate transactions properly, or produce incorrect blocks face penalties that involve the slashing of a portion of their staked ADA.
   - This provides strong economic incentives for validators to act honestly and ensures the network's integrity and security.
3. Delegation and Pool Operation:
   - Staking pools can charge operation fees (a margin on rewards) to maintain their infrastructure. This includes fixed costs set by pool operators. Delegators earn rewards after pool fees are deducted, providing a balanced incentive for both operators and delegators to participate actively.
   - Rewards are distributed at the end of each epoch, where staking pool performance and participation determine the distribution of ADA rewards to all stakeholders.

Applicable Fees:

1. Transaction Fees:
   - Transaction fees on Cardano are paid in ADA and are generally low. They are calculated based on the size of the transaction and the network's current demand. These fees are paid to validators for including transactions in new blocks.
   - The fee formula is: a + b × size, where a is a constant (typically 0.155381 ADA), b is a coefficient related to the transaction size (0.000043946 ADA/byte), and size refers to the transaction size in bytes. This ensures that the fee adapts based on network load and the size of each transaction.
2. Staking Pool Fees:
   - Staking pool operators charge operational costs and a margin fee, which covers the cost of running and maintaining the staking pool. These fees vary between pools but ensure that operators can continue to provide their services while offering rewards to delegators.
   - After the operator's fee, the remaining rewards are distributed among the delegators based on the size of their stake.

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.

Polkadot DOT

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Polkadot DOT	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/

Field	Value	Unit
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	630739.35347	kWh/a
S.10 Renewable energy consumption	27.3187045654	%
S.11 Energy intensity	0.00030	kWh
S.12 Scope 1 DLT GHG emission - Controlled	0.00000	tCO2e
S.13 Scope 2 DLT GHG emission - Purchased	186.15051	tCO2e
S.14 GHG intensity	0.00009	kgCO2e

Qualitative information

S.4 Consensus Mechanism

Polkadot DOT is present on the following networks: Binance Smart Chain, Huobi, Polkadot.

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 ensures fast block times and low fees while maintaining a level of decentralization and security.

Core Components:

1. Validators (so-called "Cabinet Members"): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network's security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.
2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security.
3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process
4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes.
5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network.
6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives
7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously.

Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB.

8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance.
9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

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.

Polkadot, a heterogeneous multi-chain framework designed to enable different blockchains to interoperate, uses a sophisticated consensus mechanism known as Nominated Proof-of-Stake (NPoS). This mechanism combines elements of Proof-of-Stake (PoS) and a layered consensus model involving multiple roles and stages.

Core Components:

1. Validators: Validators are responsible for producing new blocks and finalizing the relay chain, Polkadot's main chain. They stake DOT tokens and validate transactions, ensuring the security and integrity of the network.
2. Nominators: Nominators delegate their stake to trusted validators, choosing which validators they believe will act honestly and effectively. They share in the rewards and penalties of the validators they nominate.
3. Collators: Collators maintain parachains (individual blockchains that connect to the Polkadot relay chain) by collecting transactions from users and producing state transition proofs for validators.
4. Fishermen: Fishermen monitor the network for malicious activity. They report bad behavior to the validators to help maintain network security.

Consensus Process: Polkadot's consensus mechanism operates through a combination of two key protocols: GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement) and BABE (Blind Assignment for Blockchain Extension).

1. BABE (Block Production): BABE is the block production mechanism. It operates similarly to a lottery, where validators are pseudo-randomly assigned slots to produce blocks based on their stake. Each validator signs the blocks they produce, which are then propagated through the network.
2. GRANDPA (Finality): GRANDPA is the finality gadget that provides a higher level of security by finalizing blocks after they are produced. Unlike traditional blockchains where blocks are

considered final after a number of confirmations, GRANDPA allows for asynchronous finality. Validators vote on chains, and once a supermajority agrees, the chain is finalized instantly.

Detailed Steps:

1. Block Production (BABE):
   - Slot Allocation: Validators are selected to produce blocks in specific time slots.
   - Block Proposal: The selected validator for a slot proposes a block, including new transactions and state changes.
2. Block Propagation and Preliminary Consensus: Proposed blocks are propagated across the network, where other validators verify the correctness of the transactions and state transitions.
3. Finalization (GRANDPA):
   - Voting on Blocks: Validators vote on the chains they believe to be the correct history.
   - Supermajority Agreement: Once more than two-thirds of validators agree on a block, it is finalized.
   - Instant Finality: This finality process ensures that once a block is finalized, it is irreversible and becomes part of the canonical chain.
4. Rewards and Penalties: Validators and nominators earn rewards for participating in the consensus process and maintaining network security. Misbehavior, such as producing invalid blocks or being offline, results in penalties, including slashing of staked tokens.

S.5 Incentive Mechanisms and Applicable Fees

Polkadot DOT is present on the following networks: Binance Smart Chain, Huobi, Polkadot.

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators.

Incentive Mechanisms

1. Validators:
   - Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards.
   - Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks.
2. Delegators:
   - Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks.
   - Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network’s security and decentralization by choosing reliable validators.
3. Candidates:
   Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience.
4. Economic Security:
   - Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network.
   - Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets.

Fees on the Binance Smart Chain

1. Transaction Fees:
   - Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators.
   - Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.
2. Block Rewards:
   Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions.
3. Cross-Chain Fees:
   Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience.
4. Smart Contract Fees:
   Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

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.

Polkadot uses a consensus mechanism called Nominated Proof-of-Stake (NPoS), which involves a combination of validators, nominators, and a unique layered consensus process to secure the network:

Incentive Mechanisms:

1. Validators:
   - Staking Rewards: Validators are responsible for producing new blocks and finalizing the relay chain. They are incentivized with staking rewards, which are distributed in proportion to their stake and their performance in the consensus process. Validators earn these rewards for maintaining uptime and correctly validating transactions.
   - Commission: Validators can set a commission rate that they charge on the rewards earned by their nominators. This incentivizes them to perform well to attract more nominators.
2. Nominators:
   - Delegation: Nominators stake their tokens by delegating them to trusted validators. They share in the rewards earned by the validators they support. This mechanism incentivizes nominators to carefully choose reliable validators.
   - Rewards Distribution: The rewards are distributed among validators and their nominators based on the amount of stake contributed by each party. This ensures that both parties are incentivized to maintain the network's security.
3. Collators:
   Parachain Maintenance: Collators maintain parachains by collecting transactions and producing state transition proofs for validators. They are incentivized through rewards for their role in keeping the parachain operational and secure.
4. Fishermen:
   Monitoring: Fishermen are responsible for monitoring the network for malicious activities. They are rewarded for identifying and reporting malicious behavior, which helps maintain the network's security.
5. Economic Penalties:
   - Slashing: Validators and nominators face penalties in the form of slashing if they engage in malicious activities such as double-signing or being offline for extended periods. Slashing results in the loss of a portion of their staked tokens, which serves as a strong deterrent against bad behavior.
   - Unbonding Period: To withdraw staked tokens, participants must go through an unbonding period during which their tokens are still at risk of being slashed. This ensures continued network security even when validators or nominators decide to exit.

Fees on the Polkadot Blockchain:

1. Transaction Fees:
   - Dynamic Fees: Transaction fees on Polkadot are dynamic, adjusting based on network demand and the complexity of the transaction. This model ensures that fees remain fair and proportional to the network's usage.
   - Fee Burn: A portion of the transaction fees is burned (permanently removed from circulation), which helps to control inflation and can potentially increase the value of the remaining tokens.
2. Smart Contract Fees:
   Execution Costs: Fees for deploying and interacting with smart contracts on Polkadot are based on the computational resources required. This encourages efficient use of network resources.
3. Parachain Slot Auction Fees:
   Bidding for Slots: Projects that want to secure a parachain slot must participate in a slot auction. They bid DOT tokens, and the highest bidders win the right to operate a parachain for a specified period. This process ensures that only serious projects with significant backing can secure parachain slots, contributing to the network's overall quality and security.

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

S.15 Key energy sources and methodologies

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

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

S.16 Key GHG sources and methodologies

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

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

USDC

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	USDC	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	462659.31046	kWh/a

Qualitative information

S.4 Consensus Mechanism

USDC is present on the following networks: Algorand, Aptos Coin, Arbitrum, Avalanche, Base, Celo, Ethereum, Hedera Hbar, Linea, Near Protocol, Optimism, Polygon, Solana, Statemint, Stellar, Sui, Zksync.

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

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

The consensus process involves three stages:

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

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

Core Components:

- Parallel Execution: Transactions are processed concurrently using Block-STM, a parallel execution engine, enabling high performance and scalability.

- Leader-Based BFT: A leader is selected among validators to propose blocks, while others validate and finalize transactions.
- Dynamic Validator Rotation: Validators are rotated regularly, enhancing decentralization and preventing collusion.
- Instant Finality: Transactions achieve finality once validated, ensuring that they are irreversible.

Arbitrum is a Layer 2 solution on top of Ethereum that uses Optimistic Rollups to enhance scalability and reduce transaction costs. It assumes that transactions are valid by default and only verifies them if there's a challenge (optimistic).

Core Components:

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

Verification Process:

1. Transaction Submission: Users submit transactions to the Arbitrum Sequencer, which orders and batches them.
2. State Commitment: These batches are submitted to Ethereum with a state commitment.
3. Challenge Period: Validators have a specific period to challenge the state if they suspect fraud.
4. Dispute Resolution: If a challenge occurs, the dispute is resolved through an iterative process to identify the fraudulent transaction. The final operation is executed on Ethereum to determine the correct state.
5. Rollback and Penalties: If fraud is proven, the state is rolled back, and the dishonest party is penalized.

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

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

Avalanche Consensus Process:

1. Snowball Protocol:
   - Random Sampling: Each validator randomly samples a small, constant-sized subset of other validators.
   - Repeated Polling: Validators repeatedly poll the sampled validators to determine the preferred transaction.
   - Confidence Counters: Validators maintain confidence counters for each transaction, incrementing them each time a sampled validator supports their preferred transaction.
   - Decision Threshold: Once the confidence counter exceeds a pre-defined threshold, the transaction is considered accepted.
2. Snowflake Protocol:
   - Binary Decision: Enhances the Snowball protocol by incorporating a binary decision process. Validators decide between two conflicting transactions.
   - Binary Confidence: Confidence counters are used to track the preferred binary decision.
   - Finality: When a binary decision reaches a certain confidence level, it becomes final.

3. Avalanche Protocol:
   - DAG Structure: Uses a Directed Acyclic Graph (DAG) structure to organize transactions, allowing for parallel processing and higher throughput.
   - Transaction Ordering: Transactions are added to the DAG based on their dependencies, ensuring a consistent order.
   - Consensus on DAG: While most Proof-of-Stake Protocols use a Byzantine Fault Tolerant (BFT) consensus, Avalanche uses the Avalanche Consensus, Validators reach consensus on the structure and contents of the DAG through repeated Snowball and Snowflake.

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

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

Core Components of Celo's Consensus:

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

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

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

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

Core Components:

1. Hashgraph Consensus and aBFT:
   Hedera Hashgraph's consensus mechanism achieves aBFT, which allows the network to tolerate malicious nodes without compromising security, ensuring high levels of fault tolerance and stability.

2. Gossip about Gossip Protocol:
   The network employs a "Gossip about Gossip" protocol, where nodes share transaction information along with details of previous gossip events. This process allows each node to rapidly learn the entire network state, enhancing communication efficiency and minimizing latency.
3. Virtual Voting:
   Hedera does not rely on traditional miners or stakers. Instead, it uses virtual voting, where nodes reach consensus by analyzing the gossip history and simulating votes based on the order and frequency of transactions received. Virtual voting eliminates the need for actual voting messages, reducing network congestion and speeding up consensus.
4. Deterministic Finality:
   Once consensus is reached, transactions achieve deterministic finality instantly, making them irreversible and confirmed within seconds. This attribute is ideal for applications needing quick and irreversible transaction confirmations.
5. Staking for Network Security:
   Hedera incorporates staking to bolster network security. HBAR holders can stake their tokens to support validator nodes, contributing to the network’s resilience and encouraging long-term engagement in consensus operations.

Linea employs Zero-Knowledge Rollups (zk-Rollups) to ensure scalable, secure, and efficient transaction processing while maintaining full compatibility with the Ethereum ecosystem.

Core Components:

- Zero-Knowledge Rollups (zk-Rollups): Transactions are aggregated off-chain into batches, and a single zero-knowledge proof is submitted to the Ethereum mainnet, reducing on-chain congestion and improving scalability.
- Type 2 zkEVM: Linea is fully compatible with the Ethereum Virtual Machine (EVM), enabling seamless integration with Ethereum-based smart contracts and dApps.
- Proof Aggregation: The network employs proof aggregation to finalize multiple batches of transactions into a single zero-knowledge proof, ensuring secure and efficient finalization of Layer 2 activity on the Ethereum mainnet.

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.

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

Core Components:

1. Optimistic Rollups:
   - Rollup Blocks: Transactions are batched into rollup blocks and processed off-chain.
   - State Commitments: The state of these transactions is periodically committed to the Ethereum main chain.
2. Sequencers:
   - Transaction Ordering: Sequencers are responsible for ordering transactions and creating batches.
   - State Updates: Sequencers update the state of the rollup and submit these updates to the Ethereum main chain.
   - Block Production: They construct and execute Layer 2 blocks, which are then posted to Ethereum.
3. Fraud Proofs:
   - Assumption of Validity: Transactions are assumed to be valid by default.
   - Challenge Period: A specific time window during which anyone can challenge a transaction by submitting a fraud proof.
   - Dispute Resolution: If a transaction is challenged, an interactive verification game is played to determine its validity. If fraud is detected, the invalid state is rolled back, and the dishonest participant is penalized.

Consensus Process:

1. Transaction Submission: Users submit transactions to the sequencer, which orders them into batches.
2. Batch Processing: The sequencer processes these transactions off-chain, updating the Layer 2 state.
3. State Commitment: The updated state and the batch of transactions are periodically committed to the Ethereum main chain. This is done by posting the state root (a cryptographic hash representing the state) and transaction data as calldata on Ethereum.
4. Fraud Proofs and Challenges: Once a batch is posted, there is a challenge period during which anyone can submit a fraud proof if they believe a transaction is invalid.
   - Interactive Verification: The dispute is resolved through an interactive verification game, which involves breaking down the transaction into smaller steps to identify the exact point of fraud.

- Rollbacks and Penalties: If fraud is proven, the batch is rolled back, and the dishonest actor loses their staked collateral as a penalty.

5. Finality: After the challenge period, if no fraud proof is submitted, the batch is considered final. This means the transactions are accepted as valid, and the state updates are permanent.

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

Core Concepts:

1. Proof of Stake (PoS):
   - Validator Selection: Validators on the Polygon network are selected based on the number of MATIC tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.
   - Delegation: Token holders who do not wish to run a validator node can delegate their MATIC tokens to validators. Delegators share in the rewards earned by validators.
2. Plasma Chains:
   - Off-Chain Scaling: Plasma is a framework for creating child chains that operate alongside the main Ethereum chain. These child chains can process transactions off-chain and submit only the final state to the Ethereum main chain, significantly increasing throughput and reducing congestion.
   - Fraud Proofs: Plasma uses a fraud-proof mechanism to ensure the security of off-chain transactions. If a fraudulent transaction is detected, it can be challenged and reverted.

Consensus Process:

1. Transaction Validation:
   Transactions are first validated by validators who have staked MATIC tokens. These validators confirm the validity of transactions and include them in blocks.
2. Block Production:
   - Proposing and Voting: Validators propose new blocks based on their staked tokens and participate in a voting process to reach consensus on the next block. The block with the majority of votes is added to the blockchain.
   - Checkpointing: Polygon uses periodic checkpointing, where snapshots of the Polygon sidechain are submitted to the Ethereum main chain. This process ensures the security and finality of transactions on the Polygon network.
3. Plasma Framework:
   - Child Chains: Transactions can be processed on child chains created using the Plasma framework. These transactions are validated off-chain and only the final state is submitted to the Ethereum main chain.
   - Fraud Proofs: If a fraudulent transaction occurs, it can be challenged within a certain period using fraud proofs. This mechanism ensures the integrity of off-chain transactions.

Security and Economic Incentives:

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

2. Delegation:
   Shared Rewards: Delegators earn a share of the rewards earned by the validators they delegate to. This encourages more token holders to participate in securing the network by choosing reliable validators.
3. Economic Security:
   Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. This penalty, known as slashing, involves the loss of a portion of their staked tokens, ensuring that validators act in the best interest of the network.

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.

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

Core Components:

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

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

Core Concepts:

1. Federated Byzantine Agreement (FBA):
   - SCP is built on the principles of Federated Byzantine Agreement (FBA), which allows decentralized, leaderless consensus without the need for a closed system of trusted participants.
   - Quorum Slices: Each node in the network selects a set of other nodes (quorum slice) that it trusts. Consensus is achieved when these slices overlap and collectively agree on the transaction state.
2. Nodes and Validators:
   - Nodes: Nodes running the Stellar software participate in the network by validating transactions and maintaining the ledger.
   - Validators: Nodes that are responsible for validating transactions and reaching consensus on the state of the ledger. Consensus Process
3. Transaction Validation:
   Transactions are submitted to the network and nodes validate them based on predetermined rules, such as sufficient balances and valid signatures.

4. Nomination Phase:
   - Nomination: Nodes nominate values (proposed transactions) that they believe should be included in the next ledger. Nodes communicate their nominations to their quorum slices.
   - Agreement on Nominations: Nodes vote on the nominated values, and through a process of voting and federated agreement, a set of candidate values emerges. This phase continues until nodes agree on a single value or a set of values.
5. Ballot Protocol (Voting and Acceptance): Balloting:
   - The agreed-upon values from the nomination phase are then put into ballots. Each ballot goes through multiple rounds of voting, where nodes vote to either accept or reject the proposed values.
   - Federated Voting: Nodes exchange votes within their quorum slices, and if a value receives sufficient votes across overlapping slices, it moves to the next stage.
   - Acceptance and Confirmation: If a value gathers enough votes through multiple stages (prepare, confirm, externalize), it is accepted and externalized as the next state of the ledger.
6. Ledger Update:
   Once consensus is reached, the new transactions are recorded in the ledger. Nodes update their copies of the ledger to reflect the new state. Security and Economic Incentives
7. Trust and Quorum Slices:
   Nodes are free to choose their own quorum slices, which provides flexibility and decentralization. The overlapping nature of quorum slices ensures that the network can reach consensus even if some nodes are faulty or malicious.
8. Stability and Security:
   SCP ensures that the network can achieve consensus efficiently without relying on energy-intensive mining processes. This makes it environmentally friendly and suitable for high-throughput applications.
9. Incentive Mechanisms:
   Unlike Proof of Work (PoW) or Proof of Stake (PoS) systems, Stellar does not rely on direct economic incentives like mining rewards. Instead, the network incentivizes participation through the intrinsic value of maintaining a secure, efficient, and reliable payment network.

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

Core Components:

1. Mysten Consensus Protocol:
   - The Sui consensus is based on Mysten Labs' Byzantine Fault Tolerance (BFT) protocol, which builds on principles of Practical Byzantine Fault Tolerance (pBFT) but introduces key optimizations for performance.
   - Leaderless Design: Unlike traditional BFT models, Sui does not rely on a single leader to propose blocks. Validators can propose blocks simultaneously, increasing efficiency and reducing the risks associated with leader failure or attacks.
   - Parallel Processing: Transactions can be processed in parallel, maximizing network throughput by utilizing multiple cores and threads. This allows for faster confirmation of transactions and high scalability.
2. Transaction Validation:
   Validators are responsible for receiving transaction requests from clients and processing them. Each transaction includes digital signatures and must meet the network’s rules to be considered valid. Validators can propose transactions simultaneously, unlike many other networks that require a sequential, leader-driven process.

3. Optimistic Execution:
   Optimistic Consensus: Sui allows validators to process certain non-contentious, independent transactions without waiting for full consensus. This is known as optimistic execution and helps reduce transaction latency for many use cases, allowing for fast finality in most cases.
4. Finality and Latency:
   The system only requires three rounds of communication between validators to finalize a transaction. This results in low-latency consensus and rapid transaction confirmation times, achieving scalability while maintaining security.
5.Fault Tolerance:
   The system can tolerate up to one-third of validators being faulty or malicious without compromising the integrity of the consensus process.

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

Core Components:

- Zero-Knowledge Rollups (ZK-Rollups):
  zkSync aggregates multiple transactions off-chain and processes them in batches. A cryptographic proof, called a validity proof, is generated for each batch and submitted to the Ethereum mainnet. This ensures that all transactions are valid and compliant with Ethereum's rules without processing them individually on Layer 1.
- Validity Proofs:
  zkSync uses zk-SNARKs (Succinct Non-Interactive Arguments of Knowledge) for its validity proofs. These proofs provide mathematical guarantees that transactions within a batch are valid, eliminating the need for Ethereum nodes to re-execute off-chain transactions.
- Sequencers:
  Transactions on zkSync are ordered and processed by sequencers, which bundle transactions into batches. Sequencers maintain network efficiency and provide fast confirmations.
- Fraud Resistance:
  Unlike Optimistic Rollups, zkSync relies on validity proofs rather than fraud proofs, meaning that transactions are final and secure as soon as the validity proof is accepted by Ethereum.
- Data Availability:
  All transaction data is stored on-chain, ensuring that the network remains decentralized and users can reconstruct the state of zkSync at any time.

S.5 Incentive Mechanisms and Applicable Fees

USDC is present on the following networks: Algorand, Aptos Coin, Arbitrum, Avalanche, Base, Celo, Ethereum, Hedera Hbar, Linea, Near Protocol, Optimism, Polygon, Solana, Statemint, Stellar, Sui, Zksync.

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

1. Participation Rewards:
   - Staking Rewards: Users who participate in the consensus protocol by staking their ALGO tokens earn rewards. These rewards are distributed periodically and are proportional to the amount of ALGO staked. This incentivizes users to hold and stake their tokens, contributing to network security and stability.

- Node Participation Rewards: Validators, also known as participation nodes, are responsible for proposing and voting on blocks. These nodes receive additional rewards for their active role in maintaining the network.

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

Fees on the Algorand Blockchain

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

Incentive Mechanism:

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

Applicable Fees:

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

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

1. Validators and Sequencers:
   - Sequencers are responsible for ordering transactions and creating batches that are processed off-chain. They play a critical role in maintaining the efficiency and throughput of the network.
   - Validators monitor the sequencers' actions and ensure that transactions are processed correctly. Validators verify the state transitions and ensure that no invalid transactions are included in the batches.
2. Fraud Proofs:
   - Assumption of Validity: Transactions processed off-chain are assumed to be valid. This allows for quick transaction finality and high throughput.
   - Challenge Period: There is a predefined period during which anyone can challenge the validity of a transaction by submitting a fraud proof. This mechanism acts as a deterrent against malicious behavior.
   - Dispute Resolution: If a challenge is raised, an interactive verification process is initiated to pinpoint the exact step where fraud occurred. If the challenge is valid, the fraudulent transaction is reverted, and the dishonest actor is penalized.
3. Economic Incentives:
   - Rewards for Honest Behavior: Participants in the network, such as validators and sequencers, are incentivized through rewards for performing their duties honestly and efficiently. These rewards come from transaction fees and potentially other protocol incentives.
   - Penalties for Malicious Behavior: Participants who engage in dishonest behavior or submit invalid transactions are penalized. This can include slashing of staked tokens or other forms of economic penalties, which serve to discourage malicious actions.

Fees on the Arbitrum One Blockchain

1. Transaction Fees:
   - Layer 2 Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are typically lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
   - Arbitrum Transaction Fee: A fee is charged for each transaction processed by the sequencer. This fee covers the cost of processing the transaction and ensuring its inclusion in a batch.
2. L1 Data Fees:
   - Posting Batches to Ethereum: Periodically, the state updates from the Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee, known as the L1 data fee, which accounts for the gas required to publish these state updates on Ethereum.
   - Cost Sharing: Because transactions are batched, the fixed costs of posting state updates to Ethereum are spread across multiple transactions, making it more cost-effective for users.

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

1. Validators:

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

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

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

2. Economic Incentives:

Block Rewards: Validators receive block rewards for proposing and validating blocks. These rewards are distributed from the network's inflationary issuance of AVAX tokens.
Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This includes fees for simple transactions, smart contract interactions, and the creation of new assets on the network.

3. Penalties:

- Slashing: Unlike some other PoS systems, Avalanche does not employ slashing (i.e., the confiscation of staked tokens) as a penalty for misbehavior.Instead, the network relies on the financial disincentive of lost future rewards for validators who are not consistently online or act maliciously.
- Uptime Requirements: Validators must maintain a high level of uptime and correctly validate transactions to continue earning rewards. Poor performance or malicious actions result in missed rewards, providing a strong economic incentive to act honestly.

Fees on the Avalanche Blockchain

1. Transaction Fees:
   - Dynamic Fees: Transaction fees on Avalanche are dynamic, varying based on network demand and the complexity of the transactions. This ensures that fees remain fair and proportional to the network's usage.
   - Fee Burning: A portion of the transaction fees is burned, permanently removing them from circulation. This deflationary mechanism helps to balance the inflation from block rewards and incentivizes token holders by potentially increasing the value of AVAX over time.
2. Smart Contract Fees:
   Execution Costs: Fees for deploying and interacting with smart contracts are determined by the computational resources required. These fees ensure that the network remains efficient and that resources are used responsibly.
3. Asset Creation Fees:
   New Asset Creation: There are fees associated with creating new assets (tokens) on the Avalanche network. These fees help to prevent spam and ensure that only serious projects use the network's resources.

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

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

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

Incentive Mechanisms:

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

Applicable Fees:

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

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

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

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

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

Incentive Mechanisms:

1. Staking Rewards for Nodes:
   - HBAR Rewards for Node Operators: Node operators earn HBAR rewards for providing network security and processing transactions, incentivizing them to act honestly and support network stability.
   - User Staking: HBAR holders can stake their tokens to support nodes. Staking rewards offer an additional incentive for token holders to engage in network operations, although the structure may evolve with network growth.

2. Service-Based Node Rewards:
Nodes receive rewards based on specific services they provide to the network, such as:
- Consensus Services: Reaching consensus and maintaining transaction order.
- File Storage: Storing data on the Hedera network.
- Smart Contract Processing: Supporting contract executions for decentralized applications.

Applicable Fees:

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

Linea's incentive model aligns validator performance and network security with user needs for low-cost, efficient transaction processing.

Incentive Mechanisms:

Validator Rewards: Validators earn rewards from transaction fees for their role in processing transactions and submitting aggregated proofs to the Ethereum mainnet.

Applicable Fees:

- Transaction Fees: Users pay transaction fees in the network's native token. These fees cover the costs of executing transactions on the Layer 2 network and submitting proofs to the Ethereum mainnet.
- Cost Efficiency: zk-Rollups significantly reduce transaction fees compared to Ethereum mainnet transactions by batching multiple transactions into a single proof, making Linea an economical solution for scalable dApps.

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

Incentive Mechanisms to Secure Transactions:

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

4. Epoch Rotation and Validator Selection:
   Validators are rotated regularly during epochs to ensure fairness and prevent centralization. Each epoch reshuffles validators, allowing the protocol to balance decentralization with performance.

Fees on the NEAR Blockchain:

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

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

Incentive Mechanisms:

1. Sequencers:
   - Transaction Ordering: Sequencers are responsible for ordering and batching transactions off-chain. They play a critical role in maintaining the efficiency and speed of the network.
   - Economic Incentives: Sequencers earn transaction fees from users. These fees incentivize sequencers to process transactions quickly and accurately.
2. Validators and Fraud Proofs:
   - Assumption of Validity: In Optimistic Rollups, transactions are assumed to be valid by default. This allows for quick transaction finality.
   - Challenge Mechanism: Validators (or anyone) can challenge the validity of a transaction by submitting a fraud proof during a specified challenge period. This mechanism ensures that invalid transactions are detected and reverted.
   - Challenge Rewards: Successful challengers are rewarded for identifying and proving fraudulent transactions. This incentivizes participants to actively monitor the network for invalid transactions, thereby enhancing security.
3. Economic Penalties:
   - Fraud Proof Penalties: If a sequencer includes an invalid transaction and it is successfully challenged, they face economic penalties, such as losing a portion of their staked collateral. This discourages dishonest behavior.
   - Inactivity and Misbehavior: Validators and sequencers are also incentivized to remain active and behave correctly, as inactivity or misbehavior can lead to penalties and loss of rewards.

Fees Applicable on the Optimism Layer 2 Protocol:

1. Transaction Fees:
   - Layer 2 Transaction Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are generally lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
   - Cost Efficiency: By batching multiple transactions into a single batch, Optimism reduces the overall cost per transaction, making it more economical for users.
2. L1 Data Fees:
   - Posting Batches to Ethereum: Periodically, the state updates from Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee known as the L1 data fee, which covers the gas cost of publishing these state updates on Ethereum.
   - Cost Sharing: The fixed costs of posting state updates to Ethereum are spread across multiple transactions within a batch, reducing the cost burden on individual transactions.
3. Smart Contract Fees:
   Execution Costs: Fees for deploying and interacting with smart contracts on Optimism are based on the computational resources required. This ensures that users are charged proportionally for the resources they consume.

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

Incentive Mechanisms:

1. Validators:
   - Staking Rewards: Validators on Polygon secure the network by staking MATIC tokens. They are selected to validate transactions and produce new blocks based on the number of tokens they have staked. Validators earn rewards in the form of newly minted MATIC tokens and transaction fees for their services.
   - Block Production: Validators are responsible for proposing and voting on new blocks. The selected validator proposes a block, and other validators verify and validate it. Validators are incentivized to act honestly and efficiently to earn rewards and avoid penalties.
   - Checkpointing: Validators periodically submit checkpoints to the Ethereum main chain, ensuring the security and finality of transactions processed on Polygon. This provides an additional layer of security by leveraging Ethereum's robustness.
2. Delegators:
   - Delegation: Token holders who do not wish to run a validator node can delegate their MATIC tokens to trusted validators. Delegators earn a portion of the rewards earned by the validators, incentivizing them to choose reliable and performant validators.
   - Shared Rewards: Rewards earned by validators are shared with delegators, based on the proportion of tokens delegated. This system encourages widespread participation and enhances the network's decentralization.
3. Economic Security:
   - Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions.
   - Bond Requirements: Validators are required to bond a significant amount of MATIC tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity. Fees on the Polygon Blockchain

4. Transaction Fees:
   - Low Fees: One of Polygon's main advantages is its low transaction fees compared to the Ethereum main chain. The fees are paid in MATIC tokens and are designed to be affordable to encourage high transaction throughput and user adoption.
   - Dynamic Fees: Fees on Polygon can vary depending on network congestion and transaction complexity. However, they remain significantly lower than those on Ethereum, making Polygon an attractive option for users and developers.
5. Smart Contract Fees:
   Deployment and Execution Costs: Deploying and interacting with smart contracts on Polygon incurs fees based on the computational resources required. These fees are also paid in MATIC tokens and are much lower than on Ethereum, making it cost-effective for developers to build and maintain decentralized applications (dApps) on Polygon.
6. Plasma Framework:
   State Transfers and Withdrawals: The Plasma framework allows for off-chain processing of transactions, which are periodically batched and committed to the Ethereum main chain. Fees associated with these processes are also paid in MATIC tokens, and they help reduce the overall cost of using the network.

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.

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

Incentive Mechanisms:

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

Applicable Fees:

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

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

Incentive Mechanisms:

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

2. Intrinsic Value and Participation:
   - Network Value: The intrinsic value of participating in a secure, efficient, and reliable payment network incentivizes nodes to act honestly and maintain network security. Organizations and individuals running nodes benefit from the network's functionality and the ability to facilitate transactions.
   - Decentralization: By allowing nodes to choose their own quorum slices, Stellar promotes decentralization, reducing the risk of central points of failure and making the network more resilient to attacks. Fees on the Stellar Blockchain
3. Transaction Fees:
   - Flat Fee Structure: Each transaction on the Stellar network incurs a flat fee of 0.00001 XLM (known as a base fee). This low and predictable fee structure makes Stellar suitable for micropayments and high-volume transactions.
   - Spam Prevention: The transaction fee serves as a deterrent against spam attacks. By requiring a small fee for each transaction, Stellar ensures that the network remains efficient and that resources are not wasted on processing malicious or frivolous transactions.
4. Operational Costs:
   Minimal Fees: The minimal transaction fees on Stellar not only prevent spam but also cover the operational costs of running the network. This ensures that the network can sustain itself without placing a significant financial burden on users.
5. Reserve Requirements:
   - Account Reserves: To create a new account on the Stellar network, a minimum balance of 1 XLM is required. This reserve requirement prevents the creation of an excessive number of accounts, further protecting the network from spam and ensuring efficient resource usage.
   - Trustline and Offer Reserves: Additional reserve requirements exist for creating trustlines and offers on the Stellar decentralized exchange (DEX). These reserves help maintain network integrity and prevent abuse.

Security and Economic Incentives:

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

Fees on the SUI Blockchain:

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

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

Incentive Mechanism:

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

Applicable Fees:

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

S.9 Energy consumption sources and methodologies

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

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

Tezos

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Tezos	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/

Field	Value	Unit
S.8 Energy consumption	282247.66863	kWh/a

Qualitative information

S.4 Consensus Mechanism

Tezos is present on the following networks: Binance Smart Chain, Tezos.

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 ensures fast block times and low fees while maintaining a level of decentralization and security.

Core Components:

1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.
2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security.
3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process
4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes.
5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network.
6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives
7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB.
8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network’s security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance.
9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

Tezos operates on a Liquid Proof of Stake (LPoS) consensus mechanism, which combines flexibility in staking participation with an on-chain governance model.

Core Components:

Liquid Proof of Stake (LPoS) Tezos allows token holders to participate in staking by either directly staking their tokens or delegating them to a validator (known as a baker) without transferring ownership. Validators (bakers) are responsible for creating new blocks (baking) and endorsing other blocks for validation. Bakers and Endorsers Bakers are selected based on the amount of XTZ (Tezos tokens) staked or delegated to them. The more XTZ staked, the higher the probability of being chosen to bake or endorse blocks. Endorsers are randomly selected from a pool of bakers to validate and approve blocks baked by other bakers. This additional validation enhances network security. Self-Amendment and Governance Tezos's unique governance model allows token holders to propose, vote on, and implement network upgrades without requiring hard forks. This self-amendment protocol enables Tezos to evolve based on community and developer input, making it highly adaptable and flexible.

S.5 Incentive Mechanisms and Applicable Fees

Tezos is present on the following networks: Binance Smart Chain, Tezos.

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators.

Incentive Mechanisms

1. Validators:
   - Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards.
   - Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks.
2. Delegators:
   - Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks.
   - Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network's security and decentralization by choosing reliable validators.
3. Candidates:
   Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience.
4. Economic Security:
   - Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network.
   - Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets.

Fees on the Binance Smart Chain

1. Transaction Fees:
   - Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators.
   - Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.
2. Block Rewards:
   Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions.
3. Cross-Chain Fees:
   Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience.
4. Smart Contract Fees:
   Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

Tezos incentivizes network participation and security through baking rewards, transaction fees, and an inflationary reward model.

Incentive Mechanisms:

Rewards for Baking and Endorsing Bakers receive XTZ rewards for baking new blocks. Endorsers, who validate and approve blocks baked by others, are also rewarded in XTZ. These rewards encourage active participation and help secure the network. Delegation Incentives XTZ holders who do not wish to bake can delegate their tokens to a baker, earning a share of the baker's rewards without directly participating. This delegation option broadens participation, making it accessible to more users, thereby enhancing overall network security. Security Deposit Requirement Bakers are required to post a bond (security deposit) in XTZ to bake blocks, which is held as collateral to prevent dishonest actions. If a baker acts maliciously, they risk forfeiting this bond, creating a disincentive for bad behavior and aligning bakers' interests with network integrity.

Applicable Fees:

Transaction Fees Users pay transaction fees in XTZ for activities such as transferring funds and interacting with smart contracts. These fees are awarded to bakers and endorsers, providing them with an additional incentive to validate and secure the network. Inflationary Reward Model Tezos has an inflationary reward system, where new XTZ tokens are periodically created and distributed as rewards to bakers and endorsers. This model encourages continuous participation but gradually increases the XTZ supply, balancing network security and token availability over time.

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. 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) binance_smart_chain 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.

The following sources where used: tzStats

Cosmos ATOM

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Cosmos ATOM	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	186472.74531	kWh/a

Qualitative information

S.4 Consensus Mechanism

Cosmos ATOM is present on the following networks: Binance Smart Chain, Bitsong, Cosmos, Cronos, Ethereum, Injective, Osmosis.

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 ensures fast block times and low fees while maintaining a level of decentralization and security.

Core Components:

1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.
2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security.
3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process
4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes.
5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network.
6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives
7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB.
8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network’s security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance.
9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

BitSong operates on a Delegated Proof-of-Stake (DPoS) consensus mechanism. In this model, BTSG token holders delegate their tokens to validators, who are responsible for producing and validating new blocks. The selection of validators is based on the amount of BTSG tokens staked and the duration of staking, which determines their voting power in the network's governance processes.

The Cosmos network uses the Cosmos SDK, a modular framework that enables developers to build custom, application-specific blockchains. Cosmos SDK chains rely on Tendermint Core, a Byzantine Fault Tolerant (BFT) Proof of Stake (PoS) consensus engine that supports interoperability and fast transaction finality.

Core Components:

1. Tendermint BFT Consensus with Proof of Stake:
   - Validator Selection: Cosmos validators are selected based on the amount of ATOM they stake or receive from delegators. These validators participate in block proposal and validation through a two-thirds majority voting system.
   - Security Threshold: Tendermint BFT ensures network security as long as fewer than one-third of validators act maliciously.
2. Modular Cosmos SDK Framework:
   - Inter-Blockchain Communication (IBC): The Cosmos SDK supports IBC, allowing seamless interoperability between Cosmos-based blockchains.
   - Application Blockchain Interface (ABCI): This interface separates the consensus layer from the application layer, enabling developers to implement custom logic without modifying the consensus engine.

Cronos operates on a Proof of Stake (PoS) model integrated with Tendermint's Byzantine Fault Tolerant (BFT) consensus, designed for decentralization, security, and interoperability. This model enables validators to be selected based on staking power, rewarding them for securing and validating the network.

Core Components:

- Proof of Stake (PoS) with Tendermint BFT Validator Selection: Validators are chosen based on the amount of CRO tokens staked, securing the network and producing blocks.
- Delegation Model: Token holders can delegate their CRO to validators, enabling participation in network security without needing to run a validator node.
- Cosmos SDK and Inter-Blockchain Communication (IBC) Cross-Chain Connectivity: Built on the Cosmos SDK, Cronos enables cross-chain communication, connecting to other Cosmos blockchains and ecosystems such as Ethereum and Binance Smart Chain.

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

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

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

Core Components:

- Tendermint-based Proof of Stake (PoS):
  Ensures instant transaction finality and supports efficient block production for high-speed transactions.
- Validator Selection:
  Validators are chosen based on the amount of INJ tokens staked, considering both self-staked and delegated tokens, to maintain a decentralized network.

- Delegation:
  INJ holders can delegate their tokens to validators, earning a share of staking rewards while participating in network governance.
- Instant Finality:
  The Tendermint consensus mechanism provides immediate finality, ensuring transactions cannot be reversed once validated.

Osmosis operates on a Proof of Stake (PoS) consensus mechanism, leveraging the Cosmos SDK and Tendermint Core to provide secure, decentralized, and scalable transaction processing.

Core Components:

- Proof of Stake (PoS): Validators are chosen based on the amount of OSMO tokens they stake or are delegated by other token holders. Validators are responsible for validating transactions, producing blocks, and maintaining network security.
- Cosmos SDK and Tendermint Core: Osmosis uses Tendermint Core for Byzantine Fault Tolerant (BFT) consensus, ensuring fast finality and resistance to attacks as long as less than one-third of validators are malicious.
- Decentralized Governance: OSMO token holders can participate in governance by voting on protocol upgrades and network parameters, fostering a community-driven approach to network development.

S.5 Incentive Mechanisms and Applicable Fees

Cosmos ATOM is present on the following networks: Binance Smart Chain, Bitsong, Cosmos, Cronos, Ethereum, Injective, Osmosis.

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators.

Incentive Mechanisms

1. Validators:
   - Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards.
   - Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks.
2. Delegators:
   - Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks.
   - Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network’s security and decentralization by choosing reliable validators.
3. Candidates:
   Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience.
4. Economic Security:
   - Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network.

- Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets.

Fees on the Binance Smart Chain

1. Transaction Fees:
   - Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators.
   - Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.
2. Block Rewards:
   Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions.
3. Cross-Chain Fees:
   Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience.
4. Smart Contract Fees:
   Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

The native token, BTSG, serves multiple roles within the BitSong ecosystem, including transaction fee payments, staking, and governance participation. Validators earn rewards from transaction fees and block rewards, with a portion of these rewards distributed to delegators after deducting the validator's commission.

The Cosmos network incentivizes both validators and delegators to secure the network through staking rewards, funded by transaction fees and newly minted ATOM.

Incentive Mechanisms:

1. Staking Rewards for Validators and Delegators:
   ATOM Rewards: Validators earn staking rewards in ATOM tokens for participating in consensus, with rewards shared with delegators who stake ATOM through delegation.
2. Slashing for Accountability:
   Penalties for Misconduct: Validators who act maliciously, such as double-signing or staying offline, face slashing penalties, which remove a portion of their staked ATOM. Delegators may also experience slashing if their chosen validator is penalized, encouraging careful selection of trustworthy validators.

Applicable Fees:

1. Transaction Fees:
   User-Paid Fees in ATOM: All transactions on the Cosmos Hub incur fees paid in ATOM, compensating validators for transaction processing and helping to prevent network spam.
2. Customizable Fee Model:
   Custom Token Fees: Cosmos SDK allows individual chains to define their own transaction fees in tokens other than ATOM, supporting varied application requirements within the ecosystem.

Cronos incentivizes validators and delegators with staking rewards and transaction fees, aligning economic incentives with network security and growth.

Incentive Mechanisms:

- Staking Rewards Validators and Delegators: Both groups earn CRO rewards for supporting network security. Delegators earn a portion of the validator rewards, promoting broader network participation.
- Deflationary Mechanism Token Burning: A portion of transaction fees and staking rewards may be periodically burned, reducing CRO supply over time and potentially increasing token value.

Applicable Fees:

- Transaction and Smart Contract Fees Standard Transactions: Users pay CRO for network transactions and dApp interactions, providing a steady income for validators.
- Ethereum-Compatible Gas Fees: Executing Ethereum-compatible smart contracts incurs gas fees, similar to Ethereum, payable in CRO.

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

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

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

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

Incentive Mechanisms:

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

Applicable Fees:

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

Osmosis incentivizes validators, delegators, and liquidity providers through a combination of staking rewards, transaction fees, and liquidity incentives.

Incentive Mechanisms:

- Validator Rewards: Validators earn rewards from transaction fees and block rewards, distributed in OSMO tokens, for their role in securing the network and processing transactions. Delegators who stake their OSMO tokens with validators receive a share of these rewards.
- Liquidity Provider Rewards: Users providing liquidity to Osmosis pools earn swap fees and may receive additional incentives in the form of OSMO tokens to encourage liquidity provision.
- Superfluid Staking: Liquidity providers can participate in superfluid staking, staking a portion of their OSMO tokens within liquidity pools. This mechanism allows users to earn staking rewards while maintaining liquidity in the pools

Applicable Fees:

Transaction Fees: Users pay transaction fees in OSMO tokens for network activities, including swaps, staking, and governance participation. These fees are distributed to validators and delegators, incentivizing their continued participation and support for network security.

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. 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) binance_smart_chain, bitsong, cosmos, cronos, ethereum, injective, osmosis 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.

Polygon POL

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Polygon POL	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	92462.13088	kWh/a

Qualitative information

S.4 Consensus Mechanism

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

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

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

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

Core Concepts:

1. Proof of Stake (PoS):
   - Validator Selection: Validators on the Polygon network are selected based on the number of MATIC tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.
   - Delegation: Token holders who do not wish to run a validator node can delegate their MATIC tokens to validators. Delegators share in the rewards earned by validators.
2. Plasma Chains:
   - Off-Chain Scaling: Plasma is a framework for creating child chains that operate alongside the main Ethereum chain. These child chains can process transactions off-chain and submit only the final state to the Ethereum main chain, significantly increasing throughput and reducing congestion.
   - Fraud Proofs: Plasma uses a fraud-proof mechanism to ensure the security of off-chain transactions. If a fraudulent transaction is detected, it can be challenged and reverted.

Consensus Process:

1. Transaction Validation:
   Transactions are first validated by validators who have staked MATIC tokens. These validators confirm the validity of transactions and include them in blocks.
2. Block Production:
   - Proposing and Voting: Validators propose new blocks based on their staked tokens and participate in a voting process to reach consensus on the next block. The block with the majority of votes is added to the blockchain.
   - Checkpointing: Polygon uses periodic checkpointing, where snapshots of the Polygon sidechain are submitted to the Ethereum main chain. This process ensures the security and finality of transactions on the Polygon network.
3. Plasma Framework:
   - Child Chains: Transactions can be processed on child chains created using the Plasma framework. These transactions are validated off-chain and only the final state is submitted to the Ethereum main chain.
   - Fraud Proofs: If a fraudulent transaction occurs, it can be challenged within a certain period using fraud proofs. This mechanism ensures the integrity of off-chain transactions.

Security and Economic Incentives:

1. Incentives for Validators:
   - Staking Rewards: Validators earn rewards for staking MATIC tokens and participating in the consensus process. These rewards are distributed in MATIC tokens and are proportional to the amount staked and the performance of the validator.
   - Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This provides an additional financial incentive to maintain the network's integrity and efficiency.
2. Delegation:
   Shared Rewards: Delegators earn a share of the rewards earned by the validators they delegate to. This encourages more token holders to participate in securing the network by choosing reliable validators.
3. Economic Security:
   Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. This penalty, known as slashing, involves the loss of a portion of their staked tokens, ensuring that validators act in the best interest of the network.

S.5 Incentive Mechanisms and Applicable Fees

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

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

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

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

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

Incentive Mechanisms:

1. Validators:
   - Staking Rewards: Validators on Polygon secure the network by staking MATIC tokens. They are selected to validate transactions and produce new blocks based on the number of tokens they have staked. Validators earn rewards in the form of newly minted MATIC tokens and transaction fees for their services.
   - Block Production: Validators are responsible for proposing and voting on new blocks. The selected validator proposes a block, and other validators verify and validate it. Validators are incentivized to act honestly and efficiently to earn rewards and avoid penalties.
   - Checkpointing: Validators periodically submit checkpoints to the Ethereum main chain, ensuring the security and finality of transactions processed on Polygon. This provides an additional layer of security by leveraging Ethereum's robustness.
2. Delegators:
   - Delegation: Token holders who do not wish to run a validator node can delegate their MATIC tokens to trusted validators. Delegators earn a portion of the rewards earned by the validators, incentivizing them to choose reliable and performant validators.
   - Shared Rewards: Rewards earned by validators are shared with delegators, based on the proportion of tokens delegated. This system encourages widespread participation and enhances the network's decentralization.
3. Economic Security:
   - Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions.
   - Bond Requirements: Validators are required to bond a significant amount of MATIC tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity. Fees on the Polygon Blockchain
4. Transaction Fees:
   - Low Fees: One of Polygon's main advantages is its low transaction fees compared to the Ethereum main chain. The fees are paid in MATIC tokens and are designed to be affordable to encourage high transaction throughput and user adoption.
   - Dynamic Fees: Fees on Polygon can vary depending on network congestion and transaction complexity. However, they remain significantly lower than those on Ethereum, making Polygon an attractive option for users and developers.
5. Smart Contract Fees:
   Deployment and Execution Costs: Deploying and interacting with smart contracts on Polygon incurs fees based on the computational resources required. These fees are also paid in MATIC tokens and are much lower than on Ethereum, making it cost-effective for developers to build and maintain decentralized applications (dApps) on Polygon.
6. Plasma Framework:
   State Transfers and Withdrawals: The Plasma framework allows for off-chain processing of transactions, which are periodically batched and committed to the Ethereum main chain. Fees associated with these processes are also paid in MATIC tokens, and they help reduce the overall cost of using the network.

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.

Stellar Lumen

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	Stellar Lumen	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	52560.00000	kWh/a

Qualitative information

S.4 Consensus Mechanism

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

Core Concepts:

1. Federated Byzantine Agreement (FBA):
   - SCP is built on the principles of Federated Byzantine Agreement (FBA), which allows decentralized, leaderless consensus without the need for a closed system of trusted participants.
   - Quorum Slices: Each node in the network selects a set of other nodes (quorum slice) that it trusts. Consensus is achieved when these slices overlap and collectively agree on the transaction state.
2. Nodes and Validators:
   - Nodes: Nodes running the Stellar software participate in the network by validating transactions and maintaining the ledger.
   - Validators: Nodes that are responsible for validating transactions and reaching consensus on the state of the ledger. Consensus Process
3. Transaction Validation:
   Transactions are submitted to the network and nodes validate them based on predetermined rules, such as sufficient balances and valid signatures.
4. Nomination Phase:
   - Nomination: Nodes nominate values (proposed transactions) that they believe should be included in the next ledger. Nodes communicate their nominations to their quorum slices.
   - Agreement on Nominations: Nodes vote on the nominated values, and through a process of voting and federated agreement, a set of candidate values emerges. This phase continues until nodes agree on a single value or a set of values.
5. Ballot Protocol (Voting and Acceptance): Balloting:
   - The agreed-upon values from the nomination phase are then put into ballots. Each ballot goes through multiple rounds of voting, where nodes vote to either accept or reject the proposed values.
   - Federated Voting: Nodes exchange votes within their quorum slices, and if a value receives sufficient votes across overlapping slices, it moves to the next stage.
   - Acceptance and Confirmation: If a value gathers enough votes through multiple stages (prepare, confirm, externalize), it is accepted and externalized as the next state of the ledger.
6. Ledger Update:
   Once consensus is reached, the new transactions are recorded in the ledger. Nodes update their copies of the ledger to reflect the new state. Security and Economic Incentives
7. Trust and Quorum Slices:
   Nodes are free to choose their own quorum slices, which provides flexibility and decentralization. The overlapping nature of quorum slices ensures that the network can reach consensus even if some nodes are faulty or malicious.
8. Stability and Security:
   SCP ensures that the network can achieve consensus efficiently without relying on energy-intensive mining processes. This makes it environmentally friendly and suitable for high-throughput applications.
9. Incentive Mechanisms:
   Unlike Proof of Work (PoW) or Proof of Stake (PoS) systems, Stellar does not rely on direct economic incentives like mining rewards. Instead, the network incentivizes participation through the intrinsic value of maintaining a secure, efficient, and reliable payment network.

S.5 Incentive Mechanisms and Applicable Fees

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

Incentive Mechanisms:

1. Quorum Slices and Trust:
   - Quorum Slices: Each node in the Stellar network selects other nodes it trusts to form a quorum slice. Consensus is achieved through the intersection of these slices, creating a robust and decentralized trust network.
   - Federated Voting: Nodes communicate their votes within their quorum slices, and through multiple rounds of federated voting, they agree on the transaction state. This process ensures that even if some nodes are compromised, the network can still achieve consensus securely.
2. Intrinsic Value and Participation:
   - Network Value: The intrinsic value of participating in a secure, efficient, and reliable payment network incentivizes nodes to act honestly and maintain network security. Organizations and individuals running nodes benefit from the network's functionality and the ability to facilitate transactions.
   - Decentralization: By allowing nodes to choose their own quorum slices, Stellar promotes decentralization, reducing the risk of central points of failure and making the network more resilient to attacks. Fees on the Stellar Blockchain
3. Transaction Fees:
   - Flat Fee Structure: Each transaction on the Stellar network incurs a flat fee of 0.00001 XLM (known as a base fee). This low and predictable fee structure makes Stellar suitable for micropayments and high-volume transactions.
   - Spam Prevention: The transaction fee serves as a deterrent against spam attacks. By requiring a small fee for each transaction, Stellar ensures that the network remains efficient and that resources are not wasted on processing malicious or frivolous transactions.
4. Operational Costs:
   Minimal Fees: The minimal transaction fees on Stellar not only prevent spam but also cover the operational costs of running the network. This ensures that the network can sustain itself without placing a significant financial burden on users.
5. Reserve Requirements:
   - Account Reserves: To create a new account on the Stellar network, a minimum balance of 1 XLM is required. This reserve requirement prevents the creation of an excessive number of accounts, further protecting the network from spam and ensuring efficient resource usage.
   - Trustline and Offer Reserves: Additional reserve requirements exist for creating trustlines and offers on the Stellar decentralized exchange (DEX). These reserves help maintain network integrity and prevent abuse.

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.

ChainLink Token

Quantitative information

Field	Value	Unit
S.1 Name	Bank Frick AG	/
S.2 Relevant legal entity identifier	529900RQOBT3ZJMDRK43	/
S.3 Name of the crypto-asset	ChainLink Token	/
S.6 Beginning of the period to which the disclosure relates	2024-07-01	/
S.7 End of the period to which the disclosure relates	2025-07-01	/
S.8 Energy consumption	5018.29634	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 a Layer 2 solution on top of Ethereum that uses Optimistic Rollups to enhance scalability and reduce transaction costs. It assumes that transactions are valid by default and only verifies them if there's a challenge (optimistic).

Core Components:

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

Verification Process:

1. Transaction Submission: Users submit transactions to the Arbitrum Sequencer, which orders and batches them.
2. State Commitment: These batches are submitted to Ethereum with a state commitment.
3. Challenge Period: Validators have a specific period to challenge the state if they suspect fraud.
4. Dispute Resolution: If a challenge occurs, the dispute is resolved through an iterative process to identify the fraudulent transaction. The final operation is executed on Ethereum to determine the correct state.
5. Rollback and Penalties: If fraud is proven, the state is rolled back, and the dishonest party is penalized.

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

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

Avalanche Consensus Process:

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

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 ensures fast block times and low fees while maintaining a level of decentralization and security.

Core Components:

1. Validators (so-called "Cabinet Members"): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network's security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.
2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security.
3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process
4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being

selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes.
5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network.
6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives
7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB.
8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance.
9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

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

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

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.

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

Core Components:

1. Optimistic Rollups:
   - Rollup Blocks: Transactions are batched into rollup blocks and processed off-chain.
   - State Commitments: The state of these transactions is periodically committed to the Ethereum main chain.
2. Sequencers:
   - Transaction Ordering: Sequencers are responsible for ordering transactions and creating batches.
   - State Updates: Sequencers update the state of the rollup and submit these updates to the Ethereum main chain.
   - Block Production: They construct and execute Layer 2 blocks, which are then posted to Ethereum.
3. Fraud Proofs:
   - Assumption of Validity: Transactions are assumed to be valid by default.
   - Challenge Period: A specific time window during which anyone can challenge a transaction by submitting a fraud proof.
   - Dispute Resolution: If a transaction is challenged, an interactive verification game is played to determine its validity. If fraud is detected, the invalid state is rolled back, and the dishonest participant is penalized.

Consensus Process:

1. Transaction Submission: Users submit transactions to the sequencer, which orders them into batches.
2. Batch Processing: The sequencer processes these transactions off-chain, updating the Layer 2 state.
3. State Commitment: The updated state and the batch of transactions are periodically committed to the Ethereum main chain. This is done by posting the state root (a cryptographic hash representing the state) and transaction data as calldata on Ethereum.

4. Fraud Proofs and Challenges: Once a batch is posted, there is a challenge period during which anyone can submit a fraud proof if they believe a transaction is invalid.
   - Interactive Verification: The dispute is resolved through an interactive verification game, which involves breaking down the transaction into smaller steps to identify the exact point of fraud.
   - Rollbacks and Penalties: If fraud is proven, the batch is rolled back, and the dishonest actor loses their staked collateral as a penalty.
5. Finality: After the challenge period, if no fraud proof is submitted, the batch is considered final. This means the transactions are accepted as valid, and the state updates are permanent.

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

Core Concepts:

1. Proof of Stake (PoS):
   - Validator Selection: Validators on the Polygon network are selected based on the number of MATIC tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.
   - Delegation: Token holders who do not wish to run a validator node can delegate their MATIC tokens to validators. Delegators share in the rewards earned by validators.
2. Plasma Chains:
   - Off-Chain Scaling: Plasma is a framework for creating child chains that operate alongside the main Ethereum chain. These child chains can process transactions off-chain and submit only the final state to the Ethereum main chain, significantly increasing throughput and reducing congestion.
   - Fraud Proofs: Plasma uses a fraud-proof mechanism to ensure the security of off-chain transactions. If a fraudulent transaction is detected, it can be challenged and reverted.

Consensus Process:

1. Transaction Validation:
   Transactions are first validated by validators who have staked MATIC tokens. These validators confirm the validity of transactions and include them in blocks.
2. Block Production:
   - Proposing and Voting: Validators propose new blocks based on their staked tokens and participate in a voting process to reach consensus on the next block. The block with the majority of votes is added to the blockchain.
   - Checkpointing: Polygon uses periodic checkpointing, where snapshots of the Polygon sidechain are submitted to the Ethereum main chain. This process ensures the security and finality of transactions on the Polygon network.
3. Plasma Framework:
   - Child Chains: Transactions can be processed on child chains created using the Plasma framework. These transactions are validated off-chain and only the final state is submitted to the Ethereum main chain.
   - Fraud Proofs: If a fraudulent transaction occurs, it can be challenged within a certain period using fraud proofs. This mechanism ensures the integrity of off-chain transactions.

Security and Economic Incentives:

1. Incentives for Validators:
   - Staking Rewards: Validators earn rewards for staking MATIC tokens and participating in the consensus process. These rewards are distributed in MATIC tokens and are proportional to the amount staked and the performance of the validator.

- Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This provides an additional financial incentive to maintain the network's integrity and efficiency.

2. Delegation:
   Shared Rewards: Delegators earn a share of the rewards earned by the validators they delegate to. This encourages more token holders to participate in securing the network by choosing reliable validators.
3. Economic Security:
   Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. This penalty, known as slashing, involves the loss of a portion of their staked tokens, ensuring that validators act in the best interest of the network.

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.

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

1. Validators and Sequencers:
   - Sequencers are responsible for ordering transactions and creating batches that are processed off-chain. They play a critical role in maintaining the efficiency and throughput of the network.
   - Validators monitor the sequencers' actions and ensure that transactions are processed correctly. Validators verify the state transitions and ensure that no invalid transactions are included in the batches.
2. Fraud Proofs:
   - Assumption of Validity: Transactions processed off-chain are assumed to be valid. This allows for quick transaction finality and high throughput.
   - Challenge Period: There is a predefined period during which anyone can challenge the validity of a transaction by submitting a fraud proof. This mechanism acts as a deterrent against malicious behavior.
   - Dispute Resolution: If a challenge is raised, an interactive verification process is initiated to pinpoint the exact step where fraud occurred. If the challenge is valid, the fraudulent transaction is reverted, and the dishonest actor is penalized.
3. Economic Incentives:
   - Rewards for Honest Behavior: Participants in the network, such as validators and sequencers, are incentivized through rewards for performing their duties honestly and efficiently. These rewards come from transaction fees and potentially other protocol incentives.
   - Penalties for Malicious Behavior: Participants who engage in dishonest behavior or submit invalid transactions are penalized. This can include slashing of staked tokens or other forms of economic penalties, which serve to discourage malicious actions.

Fees on the Arbitrum One Blockchain

1. Transaction Fees:
   - Layer 2 Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are typically lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
   - Arbitrum Transaction Fee: A fee is charged for each transaction processed by the sequencer. This fee covers the cost of processing the transaction and ensuring its inclusion in a batch.
2. L1 Data Fees:
   - Posting Batches to Ethereum: Periodically, the state updates from the Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee, known as the L1 data fee, which accounts for the gas required to publish these state updates on Ethereum.
   - Cost Sharing: Because transactions are batched, the fixed costs of posting state updates to Ethereum are spread across multiple transactions, making it more cost-effective for users.

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

1. Validators:

Staking: Validators on the Avalanche network are required to stake AVAX tokens. The amount staked influences their probability of being selected to propose or validate new blocks.
Rewards: Validators earn rewards for their participation in the consensus process. These rewards are proportional to the amount of AVAX staked and their uptime and performance in validating transactions.
Delegation: Validators can also accept delegations from other token holders. Delegators share in the rewards based on the amount they delegate, which incentivizes smaller holders to participate indirectly in securing the network.

2. Economic Incentives:

Block Rewards: Validators receive block rewards for proposing and validating blocks. These rewards are distributed from the network's inflationary issuance of AVAX tokens.
Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This includes fees for simple transactions, smart contract interactions, and the creation of new assets on the network.

3. Penalties:

- Slashing: Unlike some other PoS systems, Avalanche does not employ slashing (i.e., the confiscation of staked tokens) as a penalty for misbehavior.Instead, the network relies on the financial disincentive of lost future rewards for validators who are not consistently online or act maliciously.
- Uptime Requirements: Validators must maintain a high level of uptime and correctly validate transactions to continue earning rewards. Poor performance or malicious actions result in missed rewards, providing a strong economic incentive to act honestly.

Fees on the Avalanche Blockchain

1. Transaction Fees:
   - Dynamic Fees: Transaction fees on Avalanche are dynamic, varying based on network demand and the complexity of the transactions. This ensures that fees remain fair and proportional to the network's usage.

- Fee Burning: A portion of the transaction fees is burned, permanently removing them from circulation. This deflationary mechanism helps to balance the inflation from block rewards and incentivizes token holders by potentially increasing the value of AVAX over time.

2. Smart Contract Fees:
   Execution Costs: Fees for deploying and interacting with smart contracts are determined by the computational resources required. These fees ensure that the network remains efficient and that resources are used responsibly.
3. Asset Creation Fees:
   New Asset Creation: There are fees associated with creating new assets (tokens) on the Avalanche network. These fees help to prevent spam and ensure that only serious projects use the network's resources.

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators.

Incentive Mechanisms

1. Validators:
   - Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards.
   - Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks.
2. Delegators:
   - Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks.
   - Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network's security and decentralization by choosing reliable validators.
3. Candidates:
   Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience.
4. Economic Security:
   - Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network.
   - Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets.

Fees on the Binance Smart Chain

1. Transaction Fees:
   - Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators.
   - Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.
2. Block Rewards:
   Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions.

3. Cross-Chain Fees:
   Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience.
4. Smart Contract Fees:
   Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

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

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

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

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

Incentive Mechanisms:

1. Sequencers:
   - Transaction Ordering: Sequencers are responsible for ordering and batching transactions off-chain. They play a critical role in maintaining the efficiency and speed of the network.
   - Economic Incentives: Sequencers earn transaction fees from users. These fees incentivize sequencers to process transactions quickly and accurately.
2. Validators and Fraud Proofs:
   - Assumption of Validity: In Optimistic Rollups, transactions are assumed to be valid by default. This allows for quick transaction finality.
   - Challenge Mechanism: Validators (or anyone) can challenge the validity of a transaction by submitting a fraud proof during a specified challenge period. This mechanism ensures that invalid transactions are detected and reverted.
   - Challenge Rewards: Successful challengers are rewarded for identifying and proving fraudulent transactions. This incentivizes participants to actively monitor the network for invalid transactions, thereby enhancing security.
3. Economic Penalties:
   - Fraud Proof Penalties: If a sequencer includes an invalid transaction and it is successfully challenged, they face economic penalties, such as losing a portion of their staked collateral. This discourages dishonest behavior.
   - Inactivity and Misbehavior: Validators and sequencers are also incentivized to remain active and behave correctly, as inactivity or misbehavior can lead to penalties and loss of rewards.

Fees Applicable on the Optimism Layer 2 Protocol:

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

2. L1 Data Fees:
   - Posting Batches to Ethereum: Periodically, the state updates from Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee known as the L1 data fee, which covers the gas cost of publishing these state updates on Ethereum.
   - Cost Sharing: The fixed costs of posting state updates to Ethereum are spread across multiple transactions within a batch, reducing the cost burden on individual transactions.
3. Smart Contract Fees:
   Execution Costs: Fees for deploying and interacting with smart contracts on Optimism are based on the computational resources required. This ensures that users are charged proportionally for the resources they consume.

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

Incentive Mechanisms:

1. Validators:
   - Staking Rewards: Validators on Polygon secure the network by staking MATIC tokens. They are selected to validate transactions and produce new blocks based on the number of tokens they have staked. Validators earn rewards in the form of newly minted MATIC tokens and transaction fees for their services.
   - Block Production: Validators are responsible for proposing and voting on new blocks. The selected validator proposes a block, and other validators verify and validate it. Validators are incentivized to act honestly and efficiently to earn rewards and avoid penalties.
   - Checkpointing: Validators periodically submit checkpoints to the Ethereum main chain, ensuring the security and finality of transactions processed on Polygon. This provides an additional layer of security by leveraging Ethereum's robustness.
2. Delegators:
   - Delegation: Token holders who do not wish to run a validator node can delegate their MATIC tokens to trusted validators. Delegators earn a portion of the rewards earned by the validators, incentivizing them to choose reliable and performant validators.
   - Shared Rewards: Rewards earned by validators are shared with delegators, based on the proportion of tokens delegated. This system encourages widespread participation and enhances the network's decentralization.
3. Economic Security:
   - Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions.
   - Bond Requirements: Validators are required to bond a significant amount of MATIC tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity. Fees on the Polygon Blockchain
4. Transaction Fees:
   - Low Fees: One of Polygon's main advantages is its low transaction fees compared to the Ethereum main chain. The fees are paid in MATIC tokens and are designed to be affordable to encourage high transaction throughput and user adoption.
   - Dynamic Fees: Fees on Polygon can vary depending on network congestion and transaction complexity. However, they remain significantly lower than those on Ethereum, making Polygon an attractive option for users and developers.
5. Smart Contract Fees:
   Deployment and Execution Costs: Deploying and interacting with smart contracts on Polygon incurs fees based on the computational resources required. These fees are also paid in MATIC

tokens and are much lower than on Ethereum, making it cost-effective for developers to build and maintain decentralized applications (dApps) on Polygon.

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

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.