CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG H618RN577

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified on 2026-05-04.

02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114

This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading of the crypto-asset is solely responsible for the content of this crypto-asset white paper.

03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114

This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 of the European Parliament and of the Council and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.

04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114

The crypto-asset referred to in this crypto-asset white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is "a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer". This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or service supplied solely by the issuer.

06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114

The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council or the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

Summary

07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114

Warning: This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto–asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law. This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.

08. Characteristics of the crypto-asset

The crypto-asset AAVE referred to in this white paper is a crypto-asset other than EMTs and ARTs, and is issued or represented on multiple blockchain networks, namely Binance Smart Chain, NEAR, Huobi ECO Chain, Ethereum, Polygon, Solana, Gnosis Chain and Avalanche C-Chain as of 2026-02-11 and according to DTI FFG shown in F.14. The total supply amounts to 16,000,000 units. The first activity on Binance Smart Chain can be viewed on 2021-01-29 (transaction hash: 0xa5cc7ad88fa602e2ca1eb4992369e4aff13a31a766e7f2206ed02fc7935aea9a, source: https://bscscan.com/tx/0xa5cc7ad88fa602e2ca1eb4992369e4aff13a31a766e7f2206ed02fc7935aea9a, accessed 2026-02-11). The first activity on NEAR can be viewed on 2021-04-05 (transaction hash: 23HJynXxJwzxpV4EYkdaDrbwvZXczY2qbSpYinADE7tG, source: https://nearblocks.io/txns/23HJynXxJwzxpV4EYkdaDrbwvZXczY2qbSpYinADE7tG, accessed 2026-02-11). With respect to Huobi ECO Chain, the first on-chain activity could not be identified, because the network has been taken offline in 2025. The first activity on Ethereum can be viewed on 2020-09-24 (transaction hash: 0xfd5f0c65fdea26d0b94362532554d4c6cb4935b198d75e1cc07c7df4bfd8d1ad, source: https://etherscan.io/tx/0xfd5f0c65fdea26d0b94362532554d4c6cb4935b198d75e1cc07c7df4bfd8d1ad, accessed 2026-02-11). The first activity on Polygon can be viewed on 2021-03-06 (transaction hash: 0xdfb8453b301ff22875daef7200aba5aea1ef3244b8c43437bf31c2ea8cd87ec0, source: https://polygonscan.com/tx/0xdfb8453b301ff22875daef7200aba5aea1ef3244b8c43437bf31c2ea8cd87ec0, accessed 2026-02-11). The first activity on Solana can be viewed on 2024-11-22 (transaction hash: 62ZwY912jD9jgxn37qotQkV45kbqFGXpLSAGLAfcYYXPeDP6aU9nCPuv8XyvNgnskuHw6wKPutXW48kNnLHD6YNY, source: https://solscan.io/tx/62ZwY912jD9jgxn37qotQkV45kbqFGXpLSAGLAfcYYXPeDP6aU9nCPuv8XyvNgnskuHw6wKPutXW48kNnLHD6YNY, accessed 2026-02-11). The first activity on Gnosis Chain can be viewed on 2020-11-24 (transaction hash: 0x0c60703ca34df5d847bb4fc94aea6482e875f8df5d423b64f9abc8f98b77dafb, source: https://gnosisscan.io/tx/0x0c60703ca34df5d847bb4fc94aea6482e875f8df5d423b64f9abc8f98b77dafb, accessed 2026-02-11). The first activity on Avalanche C-Chain can be viewed on 2021-07-23 (transaction hash: 0x9e50925325c298854f510e9dd93c5c1d83ef7c15a6e921b50e272251d8d899d5, source: https://subnets.avax.network/c-chain/tx/0x9e50925325c298854f510e9dd93c5c1d83ef7c15a6e921b50e272251d8d899d5, accessed 2026-02-11).

Aave is a decentralised non-custodial liquidity protocol implemented through open-source smart contracts that enable the supply and borrowing of digital assets on an over-collateralised basis. Participants may supply assets to liquidity pools and receive corresponding interest-bearing representations that accrue value algorithmically based on pool utilisation, or borrow assets subject to collateral requirements defined by protocol parameters. The protocol includes mechanisms such as flash loans executed within a single transaction block, dynamically adjusted interest rates, and modular architecture upgrades designed to coordinate liquidity across supported blockchain networks. The AAVE crypto-asset functions as a coordination and governance mechanism within this framework, enabling holders to propose and vote on protocol-level changes, including risk parameters, feature integrations and deployments. The crypto-asset may also be staked within a dedicated security module intended to act as a backstop in defined shortfall events, and may interact with incentive mechanisms and collateral configurations as defined by the protocol's smart-contract logic and governance processes.

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are purely technical or operational in nature and do not confer rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments.

09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is "a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer". This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or service supplied solely by the issuer.

10. Key information about the offer to the public or admission to trading

Crypto Risk Metrics GmbH is seeking admission to trading on Payward Global Solutions LTD ("Kraken") platform in the European Union in accordance with Article 5 of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. The admission to trading is not accompanied by a public offer of the crypto-asset.

Part A – Information about the offeror or the person seeking admission to trading

A.1 Name

Crypto Risk Metrics GmbH is the person seeking admission to trading.

A.2 Legal form

The legal form of Crypto Risk Metrics GmbH is 2HBR, which corresponds to "Gesellschaft mit beschränkter Haftung".

A.3 Registered address

The registered address of Crypto Risk Metrics GmbH is Lange Reihe 73, 20099 Hamburg,

Germany,

federal state of Hamburg.

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

Crypto Risk Metrics GmbH was registered on 2018-12-03.

A.6 Legal entity identifier

The Legal Entity Identifier (LEI) of Crypto Risk Metrics GmbH is 39120077M9TG0O1FE242.

A.7 Another identifier required pursuant to applicable national law

The national identifier of Crypto Risk Metrics GmbH is HRB 154488.

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

Crypto Risk Metrics GmbH will respond to investor enquiries within 30 calendar days.

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

Identity	Function	Business Address
Tim Zölitz	Chairman	Lange Reihe 73, 20099 Hamburg, Germany

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider that supports regulated entities in fulfilling their regulatory requirements. Among other services, Crypto Risk Metrics GmbH acts as a data provider for ESG data under Article 66(5). In light of the requirements set out in Articles 4(7), 5(4) and 66(3) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, Crypto Risk Metrics GmbH aims to provide central services for crypto-asset white papers.

A.14 Parent company business activity

Crypto Risk Metrics GmbH does not have a parent company. Accordingly, no business activity of a parent company is to be reported in this section.

A.15 Newly established

Crypto Risk Metrics GmbH has been established since 2018-12-03 and is therefore not newly established (i.e. more than three years).

A.16 Financial condition for the past three years

Crypto Risk Metrics GmbH, founded in 2018 and based in Hamburg (HRB 154488), has undergone several strategic shifts in its business focus since incorporation. Due to these changes in business model and operational direction over time, the financial figures from earlier years are only comparable to a limited extent with the company's current commercial activities. The present business model – centred on regulatory technology and risk analytics in the context of the MiCA framework – has been developed progressively and can realistically be considered fully operational since approximately 2024.

The company's financial trajectory over the past three years reflects the transition from exploratory development towards market-ready product delivery. Profit or loss after tax for the last three financial years is as follows:

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

The profit in 2022 resulted primarily from legacy consulting activities, which were discontinued as part of the company's repositioning.

The losses in 2023 and 2024 resulted from strategic investments in the development of proprietary software infrastructure, regulatory frameworks, and compliance technology for the MiCA ecosystem. During those periods, no substantial commercial revenues were expected, as resources were directed towards preparing the platform for market entry in a regulated environment.

A fundamental repositioning of the company occurred in 2023 and especially in 2024, when the focus shifted towards providing risk management, regulatory reporting, and supervisory compliance solutions for financial institutions and crypto-asset service providers. This marked a material shift in business operations and monetisation strategy.

Based on preliminary unaudited management information for the financial year 2025, revenues are expected to have exceeded EUR 800,000, while preliminary net profit is expected to exceed EUR 100,000.

These figures are not audited and are not based on a finalised annual financial statement. Accordingly, they remain subject to finalisation and may differ from the figures ultimately reported in the annual financial statements.

With the regulatory environment now taking shape and the platform commercially validated, it is assumed that the effects of the strategic developments will continue to materialise in 2026. The company foresees further scalability of its technology and growing market demand for regulatory compliance tools in the European crypto-asset sector.

No public subsidies or governmental grants have been received to date; all operations have been financed through shareholder contributions and internally generated resources. Crypto Risk Metrics has never accepted any payments in tokens from projects it has worked with and – due to its internal Conflicts of Interest Policy – never will.

A.17 Financial condition since registration

Not applicable. The company has been established for more than three years and its financial condition over the past three years is provided in Part A.16 above.

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading

B.1 Issuer different from offeror or person seeking admission to trading

Yes, the issuer is different from the person seeking admission to trading.

B.2 Name

The crypto-asset does not appear to be issued by a formal company or foundation as a legal entity. Instead, it follows a decentralised approach.

B.3 Legal form

Not applicable.

B.4 Registered address

Not applicable.

Not applicable.

Not applicable.

B.5 Head office

Not applicable.

Not applicable.

Not applicable.

B.6 Registration date

Not applicable, as the project follows a decentralised approach.

B.7 Legal entity identifier

Not applicable, as the project follows a decentralised approach.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Identity	Function	Business Address
Not applicable	Not applicable	Not applicable

B.11 Business activity

Not applicable.

B.12 Parent company business activity

Not applicable.

Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

C.1 Name

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.2 Legal form

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.3 Registered address

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.4 Head office

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.5 Registration date

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.6 Legal entity identifier

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.7 Another identifier required pursuant to applicable national law

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.8 Parent company

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.9 Reason for crypto-Asset white paper Preparation

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.10 Members of the Management body

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.11 Operator business activity

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.12 Parent company business activity

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

Not applicable, as Crypto Risk Metrics GmbH is not a trading platform.

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Aave Token", Short Name: "AAVE" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-12).

D.2 Crypto-assets name

Long Name: "Aave Token" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-12).

D.3 Abbreviation

Short Name: "AAVE" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-12).

D.4 Crypto-asset project description

According to public information (source: https://docs.aave.com/, accessed 2026-02-11), the Aave project is a crypto-asset initiative concerned with the development and operation of a decentralised, non-custodial liquidity protocol and a broader ecosystem supporting on-chain lending, borrowing, and liquidity coordination across multiple distributed-ledger networks. The protocol enables users to supply digital assets to shared liquidity pools and to borrow assets on an over-collateralised basis through self-executing smart contracts. The project is governed by a decentralised autonomous organisation and supported by independent development contributors and service providers.

The technical core of the project is the Aave Protocol, an open-source smart-contract system deployed across several blockchain networks and designed to operate as a permissionless liquidity infrastructure. The protocol supports the minting of interest-bearing derivative representations of deposited assets and employs algorithmic interest-rate models that dynamically adjust based on pool utilisation. It further incorporates risk-management configurations, such as asset-specific parameters and collateral modes, intended to manage exposure within the system.

The AAVE crypto-asset functions as an element within this broader technical framework. It is intended to interact with specific components of the protocol's internal logic, including on-chain governance procedures, staking-based security mechanisms, and selected incentive structures. Holders may propose and vote on governance actions that determine risk parameters, asset listings, protocol upgrades, and treasury allocations. In addition, AAVE may be staked within a designated safety mechanism designed to act as a financial backstop in the event of defined shortfall scenarios, subject to protocol rules and governance decisions. Certain functionalities, including staking configurations, incentive parameters, treasury management structures and

potential buyback arrangements, remain subject to ongoing technical development and future governance determinations.

The project does not involve the granting of ownership, profit-participation rights, or legal claims against the project entity or its contributors. Instead, it centres on the creation of a technical environment in which the AAVE crypto-asset may serve as a governance and utility input for certain protocol processes. The long-term evolution of the Aave system, including the scope of available features, the decentralisation roadmap, governance procedures, and the operational continuity of the infrastructure, may vary based on technical, economic, and regulatory considerations. All future developments remain subject to change.

D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project

Name of person	Type of person	Business address of person	Domicile of company
Avara Group Sezc	Other person involved in implementation	190 Elgin Avenue, KY1-9008, George Town, Cayman Islands	Cayman Islands
Aave Limited	Other person involved in implementation	71-75 Shelton Street, Covent Garden, London, England, WC2H 9JQ	United Kingdom
Peter Dennis Kerr	Other person involved in implementation	71-75, Shelton Street, Covent Garden, London, England, WC2H 9JQ	United Kingdom
Stanislav Kulechov	Other person involved in implementation	71-75, Shelton Street, Covent Garden, London, England, WC2H 9JQ	United Kingdom

D.6 Utility Token Classification

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is "a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer". This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or service supplied solely by the issuer.

D.7 Key Features of Goods/Services for Utility Token Projects

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is "a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer". This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or service supplied solely by the issuer.

D.8 Plans for the token

This section provides an overview of the historical developments related to the AAVE crypto-asset and a description of planned or anticipated project milestones as publicly communicated. All forward-looking elements are subject to significant uncertainty. They do not constitute commitments, assurances, or guarantees, and may be modified, delayed, or discontinued at any time. The implementation of past milestones cannot be assumed to continue in the future, and future changes may have adverse effects for token holders.

There is a formally published roadmap for the Aave protocol. Based on the official roadmap (sources: https://governance.aave.com/t/aave-v4-launch-roadmap/23134, https://aave.com/docs, accessed 2026-04-29), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Aave protocol and the role of the AAVE crypto-asset.

Past milestones:

- ETHLend ICO and Platform Launch (2017): The project originated as ETHLend, a peer-to-peer lending platform funded through an initial coin offering that raised approximately USD 17 million, establishing the initial economic structure later associated with the AAVE crypto-asset.

- Rebranding to Aave (Late 2018): The project transitioned from ETHLend to Aave, reconfiguring its lending model and incorporating a new parent company structure under the Aave name.

- LEND to AAVE Migration Announcement and Exchange Ratio Definition (2020): In the context of the rebranding from ETHLend to Aave and the transition to a liquidity pool-based model, the protocol announced the migration of its native crypto-asset from LEND to AAVE at a fixed exchange ratio of 100 LEND to 1 AAVE. The migration process took place during 2020 and formed part of the broader shift toward a governance structure controlled by AAVE DAO.

- Aave Version 1 Mainnet Launch (January 2020): Aave V1 was deployed on the Ethereum mainnet, introducing a liquidity pool model in place of peer-to-peer matching, as well as features such as flash loans and stable interest rate options.

- Aave Version 2 Mainnet Launch (December 2020): Aave V2 introduced debt tokenization, native credit delegation, and enhanced flash loan functionality, expanding the technical capabilities of the protocol.

- Umbrella Security Expansion (June 2025): Aave launched its "Umbrella" security module on Ethereum, transitioning from the older Safety Module to an automated, asset-specific, on-chain risk management system.

- Aave Horizon Launch (August 2025): Aave Labs launched Horizon, a marketplace focused on real-world asset markets designed for institutional participants.

- Aave Version 4 Testnet Launch (2025): Following approximately two years of development, Aave V4 was launched on testnet in 2025, enabling community testing, developer preview, and security assessments prior to production deployment.

- Aave Version 4 Mainnet Launch (2026-03-30): Aave V4 launched on Ethereum mainnet on 30 March 2026. The launch introduced a Hub and Spoke architecture, with Liquidity Hubs designed to make supplied assets available across connected Spokes with distinct collateral types, risk parameters and liquidation rules.

- rsETH incident related to the KelpDAO exploit affecting Aave markets (April 18, 2026): Following the rsETH incident connected to the KelpDAO exploit, Aave implemented a series of defensive risk-management measures across affected Aave V3 deployments. These measures included freezing rsETH and wrsETH reserves, freezing WETH in certain markets, and adjusting WETH interest-rate parameters in order to contain protocol risk and limit the potential spread of stress across reserves. Aave governance communications stated that the incident was scoped to the rsETH asset and did not stem from a vulnerability in the Aave protocol itself.

Future milestones:

- Aave App Broader Rollout (2026): The consumer-focused Aave App, currently in early access, is positioned for broader mobile adoption in 2026, subject to development progress and regulatory considerations.

- Umbrella Security Expansion (Date not specified): The protocol plans to expand the Umbrella safety module to additional Aave pools and networks, subject to governance approval and technical feasibility.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the AAVE crypto-asset for its holders.

D.9 Resource allocation

Based on information from various third-party and industry sources, it is reported that the crypto-asset project associated with the AAVE token conducted multiple funding rounds between 2017 and 2020. According to these sources, the project, originally launched under the name ETHLend, is stated to have raised approximately USD 17 million through a 2017 initial coin offering. In addition, further capital appears to have been raised through several strategic token sales and venture rounds, including a reported USD 4.5 million investment by ParaFi Capital on or around 8 July 2020, a USD 3 million token sale to Framework Ventures and Three Arrows Capital on or around 15 July 2020, and a USD 25 million strategic funding round on or around 12 October 2020 involving investors such as Blockchain Capital, Standard Crypto, and Blockchain.com Ventures.

However, this information is derived exclusively from public announcements, interviews, and third-party publications. Neither the Aave protocol nor affiliated entities such as Aave Labs have independently confirmed within the context of this white paper the precise occurrence, amounts, structure, legal classification, or contractual terms of these financing events. In particular, the available sources indicate that several of the reported funding rounds involved token purchases

rather than equity investments, while Aave Labs is described as a separate private company with its own shareholders. The exact distinction between token-based financing and private equity participation, including corresponding rights and obligations, cannot be independently verified for the purposes of this disclosure. As a result, the reported funding amounts, investor participation, structural details, and cumulative funding figures cannot be independently verified and should be considered indicative only.

D.10 Planned use of collected funds or crypto-assets

Not applicable, as this white paper serves the purpose of admission to trading and is not associated with any fundraising activity for the crypto-asset project.

Part E – Information about the offer to the public of crypto-assets or their admission to trading

E.1 Public offering or admission to trading

Crypto Risk Metrics GmbH is the person seeking admission to trading.

E.2 Reasons for public offer or admission to trading

The purpose of seeking admission to trading is to enable the crypto-asset to be listed on a regulated platform in accordance with the applicable provisions of Regulation (EU) 2023/1114 and Commission Implementing Regulation (EU) 2024/2984. The white paper has been drawn up to comply with the transparency requirements applicable to trading venues.

E.3 Fundraising target

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.4 Minimum subscription goals

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.5 Maximum subscription goals

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.6 Oversubscription acceptance

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.7 Oversubscription allocation

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.8 Issue price

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.9 Official currency or any other crypto-assets determining the issue price

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.10 Subscription fee

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.11 Offer price determination method

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.12 Total number of offered/traded crypto-assets

The maximum supply of the crypto-asset is set at 16,000,000 units. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

The admission of the crypto-asset to trading is open to all types of investors.

E.14 Holder restrictions

Holder restrictions are subject to the rules applicable to the Crypto-Asset Service Provider, as well as to any additional restrictions such provider may impose.

E.15 Reimbursement notice

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.16 Refund mechanism

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.17 Refund timeline

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.18 Offer phases

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.19 Early purchase discount

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.20 Time-limited offer

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.21 Subscription period beginning

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.22 Subscription period end

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.23 Safeguarding arrangements for offered funds/crypto-assets

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.24 Payment methods for crypto-asset purchase

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.25 Value transfer methods for reimbursement

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.26 Right of withdrawal

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.27 Transfer of purchased crypto-assets

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.28 Transfer time schedule

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.29 Purchaser's technical requirements

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.30 Crypto-asset service provider (CASP) name

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.31 CASP identifier

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.32 Placement form

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.33 Trading platforms name

The admission to trading is sought on Payward Global Solutions LTD ("Kraken").

E.34 Trading platforms Market identifier code (MIC)

The Market Identifier Code (MIC) of Payward Global Solutions LTD ("Kraken") is PGSL.

E.35 Trading platforms access

The token is intended to be listed on the trading platform operated by Payward Global Solutions LTD ("Kraken"). Access to this platform depends on regional availability and user eligibility under Kraken's terms and conditions. Investors should consult Kraken's official documentation to determine whether they meet the requirements for account creation and token trading.

E.36 Involved costs

The costs involved in accessing the trading platform depend on the specific fee structure and terms of the respective crypto-asset service provider. These may include trading fees, deposit or withdrawal charges, and network-related gas fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

E.37 Offer expenses

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.38 Conflicts of interest

MiCA-compliant crypto-asset service providers shall have strong measures in place in order to manage conflicts of interest. Due to the broad audience this white paper addresses, potential investors should always check the conflicts-of-interest policy of their respective counterparty.

Crypto Risk Metrics GmbH has established, implemented, and documented comprehensive internal policies and procedures for the identification, prevention, management, and documentation of conflicts of interest in accordance with applicable regulatory requirements. These internal measures are actively applied within the organisation. For the purposes of this specific assessment and the crypto-asset covered by this white paper, a token-specific review has been conducted by Crypto Risk Metrics GmbH. Based on this individual review, no conflicts of interest relevant to this crypto-asset have been identified at the time of preparation of this white paper.

E.39 Applicable law

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

E.40 Competent court

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCA) but is neither classified as an electronic money token (EMT) nor an asset-referenced token (ART).

It is a digital representation of value that can be stored and transferred using distributed ledger technology (DLT) or similar technology, without embodying or conferring any rights to its holder.

The asset does not aim to maintain a stable value by referencing an official currency, a basket of assets, or any other underlying rights. Instead, its valuation is entirely market-driven, based on supply and demand dynamics, and not governed by a stabilisation mechanism. It is neither pegged to any fiat currency nor backed by any external assets, thereby clearly distinguishing it from EMTs and ARTs.

Furthermore, the crypto-asset is not categorised as a financial instrument, deposit, insurance product, pension product, or any other regulated financial product under EU law. It does not grant financial rights, voting rights, or any contractual claims to its holders, ensuring that it remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

The AAVE token is designed to facilitate decentralised decision-making within the Aave Protocol. Token holders may submit governance proposals and vote on protocol-level actions, including adjustments to risk parameters, onboarding of new crypto-assets, deployment of the protocol to additional blockchain networks, and modifications to smart-contract configurations and treasury allocations. Voting rights relate exclusively to technical and protocol-level features and do not extend to decisions regarding the operation, management, or assets of Aave Labs Ltd. or other affiliated entities. Governance participation may be exercised directly or through delegated voting arrangements, subject to the applicable governance framework adopted by the Aave DAO.

Within the Aave ecosystem, AAVE may be used as a staking asset in the protocol's security module, where participants may lock AAVE as a backstop mechanism intended to mitigate potential shortfall events. In such circumstances, staked AAVE may be subject to slashing in accordance with predefined protocol rules. In return for assuming this risk, participants may receive protocol-defined incentives. AAVE may also be used as collateral within supported markets of the protocol, subject to governance-approved risk parameters, and may interact with other protocol components, including mechanisms related to the issuance and management of the GHO stablecoin. These functionalities depend on the continued operation of the Ethereum blockchain and any other distributed-ledger networks on which AAVE is deployed or bridged, the correct execution of smart contracts, governance-defined parameters, and the overall technical integrity of the protocol infrastructure.

The AAVE token does not confer ownership, profit participation, governance rights over the issuer or any related entity, or any form of economic entitlement. All functionalities are technical in nature and relate exclusively to interactions within the Aave protocol environment. The actual usability of AAVE depends on factors such as system stability, smart-contract execution, development progress, governance decisions, and the operational conditions of the Ethereum blockchain and any other distributed-ledger networks on which AAVE is deployed or bridged, which are outside the control of token holders.

F.3 Planned application of functionalities

Future milestones:

- Aave App Broader Rollout (2026): The consumer-focused Aave App, currently in early access, is positioned for broader mobile adoption in 2026, subject to development progress and regulatory considerations.

- Umbrella Security Expansion (Date not specified): The protocol plans to expand the Umbrella safety module to additional Aave pools and networks, subject to governance approval and technical feasibility.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the AAVE crypto-asset for its holders.

A description of the characteristics of the crypto asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article

F.4 Type of crypto-asset white paper

The white paper type is "Other crypto-assets" (i.e. OTHR).

F.5 The type of submission

The type of submission is MODI, which stands for "Modification".

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs and is available on multiple networks. The crypto-asset is fungible up to 18 digits after the decimal point on the Binance Smart Chain, NEAR, Huobi ECO Chain, Ethereum, Polygon, Gnosis Chain and Avalanche C-Chain networks and up to 8 digits after the decimal point on the Solana network. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. Such functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics, such as supply, demand, and liquidity in secondary markets.

F.7 Commercial name or trading name

Long Name: "Aave Token" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-12).

F.8 Website of the issuer

As no issuer is identified for the crypto-asset, there is no website of an issuer within the meaning of Regulation (EU) 2023/1114 (MiCA).

General, non-issuer-related information about the underlying project is made publicly available at: https://aave.com/.

F.9 Starting date of offer to the public or admission to trading

2026-03-20

F.10 Publication date

2026-03-20

F.11 Any other services provided by the issuer

As no issuer is identified for the crypto-asset, it cannot be excluded that additional services exist or may be offered in the future outside the scope of Regulation (EU) 2023/1114.

F.12 Language or languages of the crypto-asset white paper

EN

F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates

W6T647XQ9, WC2Q7RPJM, C36B1LTHB, F3H672QKB, S3DNT24Z3, CN6X6GTPG, 5QFJKJ1J2, R9LX080HQ

F.14 Functionally fungible group digital token identifier

H618RN577

F.15 Voluntary data flag

This white paper has been submitted as mandatory under Regulation (EU) 2023/1114.

F.16 Personal data flag

Yes, this white paper contains personal data as defined in Regulation (EU) 2016/679 (GDPR).

F.17 LEI eligibility

LEI eligibility cannot be assessed, as the issuer cannot be identified as a legal person.

F.18 Home Member State

Germany

F.19 Host Member States

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

Part G – Information on the rights and obligations attached to the crypto-assets

G.1 Purchaser rights and obligations

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers.

Any functionalities accessible through the underlying technology are of a purely technical or operational nature and do not constitute rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments.

Accordingly, holders do not acquire any claim capable of legal enforcement against the issuer or any third party.

G.2 Exercise of rights and obligations

As the crypto-asset does not establish any legally enforceable rights or obligations, there are no applicable procedures or conditions for their exercise.

Any interaction or functionality that may be available within the technical infrastructure of the project – such as participation mechanisms or protocol-level features – serves operational purposes only and does not create or constitute evidence of any contractual or statutory entitlement.

G.3 Conditions for modifications of rights and obligations

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no conditions or mechanisms under which such rights could be modified.

Adjustments to the technical protocol, smart contract logic, or related systems may occur in the ordinary course of development or maintenance.

Such changes do not alter the legal position of holders, as no contractual or regulatory rights exist. Holders should not interpret technical updates or governance-related changes as amendments to legally binding entitlements.

G.4 Future public offers

Information on the future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-02-11).

G.5 Issuer retained crypto-assets

The token does not appear to be issued by a formal company or foundation in the traditional sense. Instead, it follows a decentralised approach.

G.6 Utility token classification

No – the crypto-asset project does not concern utility tokens as defined in Article 3(9) of Regulation (EU) 2023/1114.

G.7 Key features of goods/services of utility tokens

Not applicable, as the crypto-asset described herein is not a utility token.

G.8 Utility tokens redemption

Not applicable, as the crypto-asset described herein is not a utility token.

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

Not applicable, as this white paper is written to seek admission to trading, not for the initial offer to the public.

G.11 Crypto-assets transfer restrictions

The crypto-assets themselves are not subject to any technical or contractual transfer restrictions and are generally freely transferable. However, crypto-asset service providers may impose restrictions on buyers or sellers in accordance with applicable laws, internal policies or contractual terms agreed with their clients.

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-02-11.

However, it is possible to decrease the circulating supply by transferring crypto-assets to so-called "burn addresses". These are addresses from which the tokens are no longer intended to be transferred or accessed, effectively removing them from circulation.

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 16,000,000 units according to public information (Source: https://etherscan.io/token/0x7fc66500c84a76ad7e9c93437bfc5ac33e2ddae9, 2026-02-11). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

G.14 Token value protection schemes

No – the crypto-asset does not have any mechanisms or schemes in place that aim to stabilise or protect its market value. Its value is determined solely by market supply and demand, and may be subject to significant volatility.

G.15 Token value protection schemes description

Not applicable, as the crypto-asset in scope does not have any value protection scheme in place.

G.16 Compensation schemes

No – the crypto-asset does not have any compensation scheme.

G.17 Compensation schemes description

Not applicable, as the crypto-asset in scope does not have any compensation scheme in place.

G.18 Applicable law

This white paper is submitted in the context of an application for admission to trading on a trading platform established in the European Union. Accordingly, this white paper shall be governed by the laws of the Federal Republic of Germany.

G.19 Competent court

Any disputes arising in relation to this white paper or the admission to trading may fall under the jurisdiction of the competent courts in Hamburg, Germany.

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

The crypto-asset in scope is implemented on the Ethereum, Huobi ECO Chain, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR Protocol and Avalanche networks following the standards described below.

H.2 Protocols and technical standards

The crypto-asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Huobi Token, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR Protocol and Avalanche. In general, when evaluating crypto-assets, all implementations across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Ethereum:

The crypto-asset operates on a well-defined set of protocols and technical standards that are intended to ensure its security, decentralisation, and functionality. Below are some of the key ones:

1. Network Protocols

The crypto-asset follows a decentralised, peer-to-peer (P2P) protocol where nodes communicate over the crypto-asset's DevP2P protocol using RLPx for data encoding.

- Transactions and smart contract execution are secured through Proof-of-Stake (PoS) consensus.

- Validators propose and attest blocks in Ethereum’s Beacon Chain, finalised through Casper FFG.

- The Ethereum Virtual Machine (EVM) executes smart contracts using Turing-complete bytecode.

2. Transaction and Address Standards

crypto-asset Address Format: 20-byte addresses derived from Keccak-256 hashing of public keys.

Transaction Types:

- Legacy Transactions (pre-EIP-1559)

- Type 0 (Pre-EIP-1559 transactions)

- Type 1 (EIP-2930: Access list transactions)

- Type 2 (EIP-1559: Dynamic fee transactions with base fee burning)

The Pectra upgrade introduces EIP-7702, a transformative improvement to account abstraction. This allows externally owned accounts (EOAs) to temporarily act as smart contract wallets during a transaction. It provides significant flexibility, enabling functionality such as sponsored gas payments and batched operations without changing the underlying account model permanently.

3. Blockchain Data Structure & Block Standards

- the crypto-asset's blockchain consists of accounts, smart contracts, and storage states, maintained through Merkle Patricia Trees for efficient verification.

Each block contains:

- Block Header: Parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, proposer signature.

- Transactions: Smart contract executions and token transfers.

- Block Size: No fixed limit; constrained by the gas limit per block (variable over time). In line with Ethereum's scalability roadmap, Pectra includes EIP-7691, which increases the maximum number of "blobs" (data chunks introduced with EIP-4844) per block. This change significantly boosts the data availability layer used by rollups, supporting cheaper and more efficient Layer 2 scalability.

4. Upgrade & Improvement Standards

Ethereum follows the Ethereum Improvement Proposal (EIP) process for upgrades.

The following applies to Huobi:

The HECO DAO has announced that the HECO Network (Huobi ECO Chain) will officially cease operations on January 15, 2025.

The following applies to Gnosis Chain:

Gnosis is built on the Ethereum Virtual Machine (EVM) standard and supports standards like ERC-20 and ERC-721 token protocols. Smart contracts follow widely adopted Ethereum standards, ensuring interoperability with existing tools and dApps

The following applies to Polygon:

The Polygon network is built on a clear set of protocols and standards designed to ensure scalability, interoperability, and security. Polygon is built on top of Ethereum, it combines Layer-2 features with sidechain architecture. Network security is provided through Proof-of-Stake, where validators stake POL to propose and validate blocks. The consensus architecture consists of three layers: Smart Contracts on Ethereum that are used for staking POL. The Heimdall layer consisting of Heimdall nodes running in parallel to the Ethereum mainnet, monitoring the staking smart contracts deployed on the mainnet, and committing checkpoints to the mainnet. And the Bor layer, which are block producing Bor nodes. Bor clients are based on the widely used Go Ethereum client, and therefore most technical standards on Polygon are the same as for Ethereum. Furthermore full compatibility with the Ethereum Virtual Machine (EVM) allows Ethereum smart contracts to be deployed on Polygon without modification.

The following applies to Binance Smart Chain:

Binance Smart Chain (BSC) is a Layer-1 blockchain that utilizes a Proof-of-Staked Authority (PoSA) consensus mechanism. This mechanism combines elements of Proof-of-Authority (PoA) and Proof-of-Stake (PoS) and is intended to secure the network and validate transactions. In PoSA, validators are selected based on their stake and authority, with the goal of providing fast transaction times and low fees while maintaining network security through staking.

The following applies to Solana:

The tokens were created with Solana's Token Program, a smart contract that is part of the Solana Program Library (SPL). Such tokens are commonly referred to as SPL-token. The token itself is not an additional smart contract, but what is called a data account on Solana. As the name suggests data accounts store data on the blockchain. However, unlike smart contracts, they cannot be executed and cannot perform any operations. Since one cannot interact with data accounts directly, any interaction with an SPL-token is done via Solana's Token Program. The source code of this smart contract can be found here https://github.com/solana-program/token.

The Token Program is developed in Rust, a memory-safe, high-performance programming language designed for secure and efficient development. On Solana, Rust is said to be the primary language used for developing on-chain programs (smart contracts), intended to ensure safety and reliability in decentralised applications (dApps).

Core functions of the Token Program:

initialize_mint() → Create a new type of token, called a mint

mint_to() → Mints new tokens of a specific type to a specified account

burn() → Burns tokens from a specified account, reducing total supply

transfer() → Transfers tokens between accounts

approve() → Approves a delegate to spend tokens on behalf of the owner

set_authority() → Updates authorities (mint, freeze, or transfer authority)

These functions ensure basic operations like transfers, and minting/burning can be performed within the Solana ecosystem.

In addition to the Token Program, another smart contract, the Metaplex Token Metadata Program is commonly used to store name, symbol, and URI information for better ecosystem compatibility. This additional metadata has no effect on the token's functionality.

The following applies to NEAR Protocol:

1. Network and communication protocols

NEAR is a sharded Layer-1 blockchain that uses a peer-to-peer network to distribute blocks, transaction data and state updates.

- The protocol uses the Nightshade sharding design, where multiple shards process state in parallel but jointly produce a single logical block per block height.

- Interactions between accounts and shards are handled through receipt-based asynchronous message passing, which allows cross-shard transactions without synchronous locking.

- Validators and block producers exchange block headers, chunks and receipts through NEAR's native peer-to-peer networking layer.

2. Account and addressing standards

NEAR uses a flexible, human-readable account system instead of fixed-length cryptographic addresses.

- Named accounts such as alice.near or dao.project.near act like domain names and can create hierarchical sub-accounts.

- Implicit accounts are 64-character hexadecimal addresses derived directly from a public key.

- Ethereum-style 0x addresses are also supported, allowing compatibility with Ethereum wallets such as MetaMask.

3. Access key and permission model

NEAR accounts can contain multiple cryptographic keys with different permissions.

- Full-access keys allow complete control of an account, including transfers, contract deployment and key management.

- Function-call keys are restricted and can only call specific smart-contract methods and cannot transfer NEAR or modify ownership.

This allows fine-grained security and enables wallet delegation and application-specific permissions.

4. Cryptographic and security standards

NEAR uses standard cryptographic primitives to secure accounts, transactions and validator assignments.

- Ed25519 is used for public-private key pairs and transaction signatures.

- A Verifiable Random Function (VRF) is used to assign validators to shards in an unpredictable way, reducing the risk of targeted attacks.

- Erasure-coded data distribution ensures that block data can be reconstructed even if some producers are offline or malicious.

5. Transaction, asset and data standards

- The native NEAR token is used for transaction fees, storage deposits and protocol-level accounting.

- NEAR Enhancement Proposals (NEPs) define protocol-level standards.

- NEP-366 enables meta-transactions via DelegateActions, allowing third parties to pay transaction fees on behalf of users.

- NEP-536 defines how unused gas is refunded to improve execution efficiency.

- Blockchain data, transactions and contract state are serialized using Borsh, a compact and deterministic binary format optimized for hashing and storage.

6. Storage and state accounting

NEAR applies a storage staking model.

- Accounts must lock NEAR tokens proportional to the amount of on-chain data they store, at a rate of approximately 1 NEAR per 100 kB.

- This ensures that long-term state storage is paid for by the parties that consume it.

7. Smart-contract execution

Smart contracts are executed in a deterministic runtime.

- Contracts run as WebAssembly (WASM) bytecode.

- Contract calls and cross-contract interactions are executed through receipt-based message passing.

- Execution results are deterministic so that all nodes reach the same outcome.

The following applies to Avalanche:

The crypto-asset is implemented on the Avalanche C-Chain, which is the smart contract chain of the Avalanche Primary Network. The C-Chain is a decentralised distributed-ledger environment designed to support token transfers, smart-contract execution, and interaction with Ethereum-compatible applications and tooling. The network relies on a defined set of protocols, execution standards, cryptographic primitives, and networking interfaces intended to support deterministic processing, validator coordination, and interoperability within the Avalanche ecosystem. The most relevant protocols and technical standards are outlined below.

1. Network architecture and core protocols

The Avalanche C-Chain is a linear blockchain operated within the Avalanche Primary Network. It runs the Coreth virtual machine, which is Avalanche's implementation of the Ethereum Virtual Machine and is designed to support Solidity-based smart contracts and compatibility with Ethereum tooling. Consensus on the C-Chain is achieved through Snowman++, implemented through the ProposerVM wrapper, which introduces stake-weighted proposer windows for block production while preserving the underlying Snowman consensus model for linear chains. In addition, Avalanche has introduced a formal standards process through Avalanche Community Proposals (ACPs), while relevant Ethereum Improvement Proposals (EIPs) are also incorporated where adopted by the C-Chain's EVM-compatible execution environment, including EIP-1559 transaction fee mechanics and later Ethereum upgrades such as Cancun-related changes.

2. Transaction, execution and state standards

Transactions and state transitions on the C-Chain follow an account-based model consistent with EVM operation. Coreth executes EVM bytecode and maintains blockchain state through Merkle Patricia Tree structures backed by PebbleDB or LevelDB through AvalancheGo's database interface. For atomic transaction formats, Avalanche documentation identifies the Coreth transaction format as the canonical reference for serialisation, and transaction identifiers are derived as the SHA256 hash of the signed transaction bytes. The execution layer further applies EIP-1559 base fee rules for dynamic fee calculation. Avalanche has also documented a proposed architectural change through ACP-194, termed Streaming Asynchronous Execution, under which consensus and execution may be decoupled by placing accepted transactions into a queue for delayed concurrent execution.

3. Address, cryptographic and validation standards

The C-Chain relies on established cryptographic primitives for transaction authentication and validator identification. User transaction signing is based on the secp256k1 elliptic curve standard used throughout EVM systems. Validator operations additionally rely on BLS public keys and proofs of possession in the Avalanche staking framework. The chain also uses SHA256 hashing for transaction identifiers, while state and receipt commitments are maintained through Merkle Patricia Trees. These cryptographic mechanisms form the basis for transaction authentication, validator identity, and verifiable state commitment within the network.

4. Networking and interface standards

Validator nodes on Avalanche communicate through a peer-to-peer networking layer using two-way authenticated TLS connections based on staking certificates, from which node identifiers are derived. External peer connectivity is conducted through the staking port, which is 9651 by default. For developer and wallet interaction, the C-Chain exposes JSON-RPC and WebSocket interfaces, including standard Ethereum-compatible namespaces such as eth, net, and web3, with optional support for additional namespaces such as debug. These interfaces are intended to support interoperability with wallets, indexers, developer tooling, and other infrastructure services operating in an EVM-compatible environment.

5. Protocol development and improvement standards

Technical modifications to Avalanche are proposed and discussed through the Avalanche Community Proposal process. This process covers standards-track, meta, and best-practice changes. Relevant protocol modifications affecting the C-Chain include ACP-194 on Streaming Asynchronous Execution and ACP-267 concerning validator uptime requirements. Because the C-Chain is EVM-compatible, changes in Ethereum standards may also be incorporated through updates to Coreth and AvalancheGo, subject to network adoption.

H.3 Technology used

The crypto-asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Huobi Token, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR Protocol and Avalanche. In general, when evaluating crypto-assets, all implementations across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Ethereum:

1. Decentralised Ledger: The Ethereum blockchain acts as a decentralised ledger for all token transactions, with the intention to preserve an unalterable record of token transfers and ownership to ensure both transparency and security.

2. Private Key Management: To safeguard their token holdings, users must securely store their wallet's private keys and recovery phrases.

3. Cryptographic Integrity: Ethereum employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers. The Keccak-256 (SHA-3 variant) Hashing Algorithm is used for hashing and address generation. The crypto-asset uses ECDSA with secp256k1 curve for key generation and digital signatures. Next to that, BLS (Boneh-Lynn-Shacham) signatures are used for validator aggregation in PoS.

The following applies to Huobi:

The HECO DAO has announced that the HECO Network (Huobi ECO Chain) will officially cease operations on January 15, 2025.

The following applies to Gnosis Chain:

Gnosis uses an Ethereum-compatible architecture focused on efficient governance and DAO applications. By employing Rollups and an energy-efficient infrastructure, scalability and transaction performance are enhanced.

The following applies to Polygon:

Polygon operates as a decentralised ledger that records all token transactions on its network, ensuring transparency and security through an immutable record of transfers and ownership. To protect their holdings, users must securely manage their private keys and recovery phrases, since access to tokens depends entirely on these credentials.

The network relies on elliptic curve cryptography for secure transaction validation and execution. Polygon uses the secp256k1 curve with ECDSA for key generation and digital signatures, while the Keccak-256 hashing algorithm underpins address derivation and transaction integrity. This combination of cryptographic standards provides the foundation for both the security and reliability of the Polygon ecosystem.

Polygon's Bor client is based on Ethereum's Go Ethereum Client. Polygon's Heimdall client is built using Cosmos-SDK and CometBFT.

The following applies to Binance Smart Chain:

1. BSC-Compatible Wallets

Tokens on BSC are supported by wallets compatible with the Ethereum Virtual Machine (EVM), such as MetaMask. These wallets can be configured to connect to the BSC network and are designed to interact with BSC using standard Web3 interfaces.

2. Ledger

BSC maintains its own decentralised ledger for recording token transactions. This ledger is intended to ensure transparency and security, providing a verifiable record of all activities on the network.

3. BEP-20 Token Standard

BSC supports tokens implemented under the BEP-20 standard, which is tailored for the BSC ecosystem. This standard is designed to facilitate the creation and management of tokens on the network.

4. Scalability and Transaction Efficiency

BSC is designed to handle high volumes of transactions with low fees. It leverages its PoSA consensus mechanism to achieve fast transaction times and efficient network performance, making it suitable for applications requiring high throughput.

The following applies to Solana:

1. Solana-Compatible Wallets: The tokens are supported by all wallets compatible with Solana's Token Program

2. Decentralised Ledger: The Solana blockchain acts as a decentralised ledger for all token transactions, with the intention to preserve an unalterable record of token transfers and ownership to ensure both transparency and security.

3. SPL Token Program: The SPL (Solana Program Library) Token Program is an inherent Solana smart contract built to create and manage new types of tokens (so called mints). This is significantly different from ERC-20 on Ethereum, because a single smart contract that is part of Solana's core functionality and as such is open source, is responsible for all the tokens. This ensures a high uniformity across tokens at the cost of flexibility.

4. Blockchain Scalability: With its intended capacity for processing a lot of transactions per second and in most cases low fees, Solana is intended to enable efficient token transactions, maintaining high performance even during peak network usage.

Security Protocols for Asset Custody and Transactions:

1. Private Key Management: To safeguard their token holdings, users must securely store their wallet's private keys and recovery phrases.

2. Cryptographic Integrity: Solana employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers.

The following applies to NEAR Protocol:

1. Decentralised ledger

- The NEAR blockchain acts as a decentralised ledger that records all NEAR token transfers and smart-contract interactions.

2. Smart-contract execution environment

- NEAR uses a runtime layer based on WebAssembly (WASM) to execute smart contracts.

- Smart contracts run in an isolated and deterministic environment, ensuring that all network participants compute the same result from the same inputs.

3. Token and application standards

- The NEAR ecosystem supports native fungible tokens (FTs) and non-fungible tokens (NFTs) defined through NEAR Enhancement Proposals (NEPs).

- NEP-366 enables meta-transactions, allowing transactions to be submitted on behalf of users by third-party relayers, supporting gas-sponsored interactions and easier onboarding.

The following applies to Avalanche:

1. Decentralised ledger: The Avalanche C-Chain operates as a decentralised account-based blockchain that records token transfers, smart-contract interactions, and related state changes in a linear chain structure intended to preserve an ordered and verifiable record of transactions.

2. EVM-compatible smart-contract environment: The C-Chain uses Coreth, Avalanche's implementation of the Ethereum Virtual Machine, and supports the deployment and execution of smart contracts, including contracts written in Solidity, in a manner designed to remain compatible with Ethereum developer tools and infrastructure.

3. Cryptographic integrity and state storage: The network uses secp256k1 cryptography for user transaction signing, SHA256 for transaction identifiers, and Merkle Patricia Trees for state and receipt commitments, with chain state stored through PebbleDB or LevelDB in the AvalancheGo environment.

4. Cross-chain functionality within Avalanche: The C-Chain supports atomic import and export transactions with the Avalanche X-Chain and P-Chain through shared memory mechanisms, and the broader architecture also supports interaction with Avalanche L1s.

H.4 Consensus mechanism

The crypto-asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Huobi Token, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR Protocol and Avalanche. In general, when evaluating crypto-assets, all implementations across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Ethereum:

Ethereum'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, and a validator is randomly selected to propose each new block. Once proposed, the other validators verify the block's integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalisation 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 behaviour or inactivity. PoS aims to improve energy efficiency, security, and scalability, with upgrades such as Proto-Danksharding (EIP-4844) already implemented to enhance Layer 2 scalability and transaction efficiency.

The following applies to Huobi:

Disclaimer: The HECO DAO has announced that the HECO Network (Huobi ECO Chain) will officially cease operations on January 15, 2025.

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

Key Features of HECO's Consensus Mechanism:

1. Validator Selection: HECO supports up to 21 validators, selected based on their stake in the network.

2. Transaction Processing: Validators are responsible for processing transactions and adding blocks to the blockchain.

3. Transaction Finality: The consensus mechanism ensures quick finality, allowing for rapid confirmation of transactions.

4. Energy Efficiency: By utilizing PoS elements, HECO reduces energy consumption compared to traditional Proof-of-Work systems.

The following applies to Gnosis Chain:

Gnosis operates with a Proof-of-Stake (PoS) consensus mechanism, where validators secure the network by staking GNO tokens and participating in block production.

The following applies to Polygon:

Polygon is a scaling solution for Ethereum that stores and process transaction data on its own separate chain and regularly submits checkpoints to Ethereum. This type of scaling solution is sometimes referred to as a plasma chain, and is distinct from sidechains, which don’t store checkpoints and Layer 2 solutions that store all transaction data on Ethereum in addition to the checkpoints. 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 POL tokens they have staked. The more tokens are 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 POL tokens to validators. Delegated tokens also count towards the block production chance of the validator they are delegated to. Delegators receive a share of rewards earned by validators.

Consensus Process

2. Transaction Validation: Transactions are first validated by validators who have staked POL tokens. These validators confirm the validity of transactions and include them in blocks.

3. Block Production: Proposing and Voting: Validators are randomly selected to propose new blocks. Their selection chance is proportional to their staked tokens. Validators also participate in a voting process to reach consensus on the next block. The block with most votes is added to the blockchain. Checkpointing: Polygon uses periodic checkpointing, where a cryptographic summary of the transactions on the Polygon chain is submitted to the Ethereum main chain. This process ensures the security and finality of transactions on the Polygon network.

The following applies to Binance Smart Chain:

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 decentralisation 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 decentralisation 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, incentivising 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 decentralisation.

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 behaviour. This staked amount can be slashed if validators act maliciously. Staking incentivises 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 incentivises 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 incentivising them to validate transactions accurately and efficiently.

The following applies to Solana:

Solana uses a combination of Proof-of-History (PoH) and Proof-of-Stake (PoS). The core concepts of the mechanism are intended to work as follows:

Core Concepts

1. Proof-of-History (PoH):

PoH is a cryptographic ordering and timing mechanism that provides evidence that data existed in a particular sequence and that time passed between proofs.

Verifiable Delay Function (VDF): PoH relies on a sequential hash-based proof process that Solana describes as VDF-like. 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: Leader slots are assigned through the network's leader schedule, which is stake-weighted. The more SOL 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 contributing to the network's security.

Consensus Process

1. Transaction Validation:

Transactions are broadcasted 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 Finalisation:

Other validators vote on the ledger state associated with the block. A block may first become confirmed and later finalised once it reaches the network's strongest confirmation state.

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: Staking provides economic alignment, and Solana documentation notes that slashing has been discussed as a future mechanism for intentional malicious behaviour, but is not implemented yet.

Delegated Staking: Token holders can delegate their SOL tokens to validators, intended to enhance network security and decentralisation. Delegators share in the rewards and are incentivised to choose reliable validators.

3. Economic Penalties:

Slashing (planned): Validators can be penalized for malicious behaviour, 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.

The following applies to NEAR Protocol:

1. Core consensus model

- NEAR does not use miners; instead, it relies on validators that stake NEAR tokens to participate in block and chunk production.

- Nightshade is a sharded consensus model in which all shards jointly produce a single logical block for each block height.

- Each shard produces a chunk containing transactions and state changes for that shard, and a designated block producer aggregates all chunks into one block.

2. Validator roles

- Block and Chunk Producers are responsible for creating blocks and producing shard chunks.

- Chunk Validators verify the correctness of chunks produced by other validators.

- Hidden Validators are randomly assigned to shards using a Verifiable Random Function (VRF) and verify chunk correctness without their assignment being known in advance.

- Fishermen are observing nodes that monitor the network and can submit fraud proofs if invalid behaviour is detected.

3. Block production and finality

- Blocks and chunks are produced at an interval of approximately one second.

- Transactions become final once all related receipts (cross-shard execution messages) have been processed.

- Most transactions reach finality within 1 to 3 seconds, depending on cross-shard execution.

The following applies to Avalanche:

The Avalanche C-Chain uses the Snowman++ consensus mechanism, which is Avalanche's consensus model for linear blockchains and is implemented through the ProposerVM wrapper. Under this model, validators repeatedly query a small random subset of other validators and converge on a preferred block once the required confidence thresholds are met. Avalanche documentation describes the baseline Snowman parameters with a sample size of k = 20, quorum threshold α = 14, and decision threshold β = 20, while also noting that the AvalancheGo implementation includes additional optimisations for latency and throughput.

Only Primary Network validators are entitled to validate the C-Chain. To participate as a validator on Avalanche mainnet, a node must stake a minimum of 2,000 AVAX for a period of 14 to 365 days. Token holders may also participate indirectly by delegating at least 25 AVAX to an existing validator. Validator identity and admission to staking require the relevant staking credentials, including BLS proofs of possession under the current staking framework.

For block production, Snowman++ uses stake-weighted proposer windows. Through the ProposerVM, block-building opportunities are assigned to proposers in 5-second windows, after which block production may fall back more broadly to validators if necessary. This mechanism is intended to regulate block production while preserving network liveness. Consensus voting itself remains based on repeated sub-sampled polling rather than fixed validator committees.

Avalanche documentation describes the finality model as sub-second and treated by the protocol as final and irreversible once accepted, while noting that safety is probabilistic in the formal sense because the probability of conflicting acceptance can be reduced to an arbitrarily low level through the protocol parameters. The protocol does not rely on slashing of staked principal. Instead, validator reward eligibility depends on compliance with protocol conditions, including uptime requirements. Under current Avalanche documentation, the validator uptime threshold for reward eligibility is 90%, following ACP-267.

H.5 Incentive mechanisms and applicable fees

The crypto-asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Huobi Token, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR Protocol and Avalanche. In general, when evaluating crypto-assets, all implementations across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Ethereum:

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.

The following applies to Huobi:

Disclaimer: The HECO DAO has announced that the HECO Network (Huobi ECO Chain) will officially cease operations on January 15, 2025.

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.

The following applies to Gnosis Chain:

Validators on Gnosis earn GNO rewards for validating transactions and securing the network. Transaction fees are used to compensate for network resources and maintain stability.

The following applies to Polygon:

Incentive Mechanisms

1. Validators: Staking Rewards: Validators on Polygon secure the network by staking POL tokens. Validators are rewarded for block production and block validation/voting. They earn rewards in the form of newly minted POL tokens and, when they produce blocks, some transaction fees.

2. Delegators: Delegation: Token holders who do not wish to run a validator node can delegate their POL tokens to trusted validators. Delegators earn a portion of the rewards earned by the validators, incentivising them to choose reliable and performant validators. Validators profit from delegations, because their chance of being selected for block production and therefore the associated expected rewards increase. This system encourages widespread participation and enhances the network's decentralisation.

3. Economic Security: Slashing: Validators can be penalised through a process called slashing if they engage in malicious behaviour 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 POL tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity.

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

The following applies to Binance Smart Chain:

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivise 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 incentivises token holders to participate in the network's security and decentralisation 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 penalised for malicious behaviour 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

5. 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.

6. Block Rewards: Incentivising 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.

7. 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.

8. Smart Contract Fees: Deployment and Execution Costs: 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 following applies to Solana:

1. Validators:

Validators participate in block production and voting under Solana's stake-weighted model. They may receive staking-related rewards and a share of transaction-fee income. Under Solana's fee model, the base fee is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This is intended to provide 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 the rewards earned by the validators. This is intended to encourage widespread participation in securing the network and to support decentralisation.

3. Economic Security:

Solana staking documentation notes slashing as a possible future mechanism for intentional malicious conduct, but states that slashing is not implemented in the protocol today. Economic alignment instead currently arises primarily from staking participation, validator performance incentives, and the opportunity cost of locking capital in staking positions.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana transactions require fees in SOL. The fee model consists of a base fee and, where used, an optional prioritisation fee. The base fee compensates signature verification work and is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

2. Rent Fees:

Solana accounts that store on-chain state must satisfy the rent-exemption threshold, which is linked to the amount of data stored. This mechanism is intended to support efficient use of network state and account storage resources.

3. Program Execution Costs:

Deploying and interacting with on-chain programs may involve transaction fees and, where relevant, compute-related prioritisation fees and account-storage requirements. These mechanisms are intended to allocate network resources in proportion to use.

The following applies to NEAR Protocol:

1. Validator incentives

- Validators must stake NEAR tokens in order to participate in block and chunk production.

- Validators receive epoch rewards every epoch (approximately 12 hours, or 43,200 blocks).

- The protocol targets an annual validator reward rate of approximately 2.5% to 4.5% of the total token supply, depending on how much NEAR is staked across the network.

- Rewards are socialized, meaning validators are paid based on their stake rather than the number of transactions or shards they directly process.

- Maximum annual protocol inflation is capped at 5%, of which 4.5% is used for validator rewards and 0.5% is allocated to the Protocol Treasury.

2. Transaction fees and fee burning

- Transaction fees on NEAR are paid in NEAR tokens.

- 100% of gas fees (after the developer rebate) are burned, permanently removing those tokens from circulation.

- 30% of the gas fees generated by a smart-contract call are automatically paid to the contract account as a developer rebate.

- Fee burning offsets inflation and may make the token supply deflationary during periods of high network usage.

3. Developer incentives

- Developers earn 30% of the gas fees generated when users interact with their smart contracts.

- These rewards are paid directly and automatically by the protocol, allowing developers to monetize applications without issuing their own tokens.

4. Storage staking incentives

- Users and developers must stake NEAR tokens to store data on-chain.

- The storage cost is approximately 1 NEAR per 100 kB of state.

- Tokens locked for storage cannot be used for validation staking, reducing the total circulating supply and indirectly increasing validator yields.

5. Slashing and economic penalties

- Validators risk losing their staked NEAR if they misbehave.

- Double signing results in progressive slashing, up to the full stake if a large portion of validators misbehave.

- Producing an invalid chunk results in 100% slashing of the validator's stake.

- Validators that confirm erasure-coded land mines are immediately slashed.

- Validators that fail to meet production requirements can be removed from the active set through kickout thresholds.

6. Fishermen and protocol treasury

- Fishermen monitor the network and submit fraud proofs. They must post a 10 NEAR bond, which is lost if they submit false challenges.

- 10% of protocol inflation (approximately 0.5% of total supply per year) is allocated to a Protocol Treasury used to fund ecosystem development, infrastructure and education.

The following applies to Avalanche:

The Avalanche C-Chain is secured economically through the native AVAX token. Validator incentives are based primarily on staking rewards, not on redistribution of C-Chain transaction fees. A fixed amount of 360 million AVAX was minted at genesis, while additional AVAX is minted over time as validator rewards, subject to Avalanche's capped token supply framework. Validator rewards are paid at the end of the staking period and are determined by factors such as the validator's stake and compliance with staking conditions.

Unlike some proof-of-stake systems, the Avalanche Primary Network does not use slashing of bonded principal as an ordinary penalty mechanism. Instead, the main protocol-level economic consequence for underperformance is the loss of reward eligibility. Where a validator fails to satisfy the applicable uptime requirement during its staking term, that validator does not receive the corresponding staking reward. In current Avalanche documentation, the required uptime level for reward eligibility is 90%.

Transaction fees apply on the C-Chain for transfers and smart-contract execution. The fee model follows EIP-1559 logic, meaning that transactions are priced through a dynamic base fee mechanism. In contrast to Ethereum's validator tip model, C-Chain transaction fees are burned rather than distributed to validators. This means that C-Chain fees function as a supply-reduction mechanism and are intended in part to offset inflation arising from the minting of validator rewards.

In addition to ordinary transaction and smart-contract execution fees, Avalanche documentation also recognises protocol fees in connection with other network operations on other chains of the Primary Network, such as certain import or export operations and staking-related actions. However, for the C-Chain itself, the core applicable fee category is the gas fee for transaction inclusion and contract execution, and those fees are handled through the protocol burn mechanism rather than paid to validators or a treasury.

H.6 Use of distributed ledger technology

No – DLT is not operated by the issuer, the offeror, the person seeking admission to trading, or any third-party acting on their behalf.

H.7 DLT functionality description

Not applicable, as the DLT is not operated by the issuer, the offeror, the person seeking admission to trading, or any third-party acting on their behalf.

H.8 Audit

As the term "technology" encompasses a broad range of components, it cannot be confirmed that all elements or aspects of the technology employed have undergone a comprehensive and systematic technical examination. Accordingly, the answer to whether an audit of the technology used has been conducted must be no. This white paper focuses primarily on risk-related aspects and therefore does not imply, nor should it be interpreted as implying, that a full assessment or audit of all technological elements has been conducted.

H.9 Audit outcome

Not applicable, as no comprehensive audit of the technology used has been conducted or can be confirmed.

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

Regulatory frameworks applicable to crypto-asset services in the European Union and in third countries are evolving. Supervisory authorities may introduce, interpret, or enforce rules that affect (i) the eligibility of this crypto-asset for admission to trading, (ii) the conditions under which a crypto-asset service provider may offer trading, custody, or transfer services for it, or (iii) the persons or jurisdictions to which such services may be provided. As a result, the crypto-asset service provider admitting this crypto-asset to trading may be required to suspend, restrict, or terminate trading or withdrawals for regulatory reasons, even if the crypto-asset itself continues to function on its underlying network.

2. Trading venue and connection risk

Trading in the crypto-asset depends on the uninterrupted operation of the trading platform admitting it and, where applicable, on its technical connections to external liquidity sources or venues. Interruptions such as system downtime, maintenance, faulty integrations, API changes, or failures at an external venue can temporarily prevent order placement, execution, deposits, or withdrawals, even when the underlying blockchain is functioning. In addition, trading platforms in emerging markets may operate under differing governance, compliance, and oversight standards, which can increase the risk of operational failures or disorderly market conditions.

3. Market formation and liquidity conditions

The price and tradability of the crypto-asset depend on actual trading activity on the venues to which the service provider is connected, whether centralised exchanges (CEXs) or decentralised exchanges (DEXs). Trading volumes may at times be low, order books thin, or liquidity concentrated on a single venue. In such conditions, buy or sell orders may not be executed in full or may be executed only at a less favourable price, resulting in slippage.

Volatility: The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the crypto-asset at or close to a previously observed price, even though no negative project-specific event has occurred.

4. Counterparty and service-provider dependence

The admission of the crypto-asset to trading may rely on several external parties, such as connected centralised or decentralised trading venues, liquidity providers, brokers, custodians, or technical integrators. If any of these counterparties fail to perform, suspend their services, or apply internal restrictions, the trading, deposit, or withdrawal of the crypto-asset on the admitting service provider can be interrupted or halted.

Quality of counterparties: Trading venues and service providers in certain jurisdictions may operate under regulatory or supervisory standards that are lower or differently enforced than those applicable in the European Union. In such environments, deficiencies in governance, risk management, or compliance may remain undetected, which increases the probability of abrupt service interruptions, investigations, or forced wind-downs.

Delisting and service suspension: The crypto-asset's availability may depend on the internal listing decisions of these counterparties. A delisting or suspension on a key connected venue can materially reduce liquidity or make trading temporarily impossible on the admitting service provider, even if the underlying crypto-asset continues to function.

Insolvency of counterparties: If a counterparty involved in holding, routing, or settling the crypto-asset becomes insolvent, enters restructuring, or is otherwise subject to resolution-type measures, assets held or processed by that counterparty may be frozen, become temporarily unavailable, or be recoverable only in part or not at all, which can result in losses for clients whose positions were

maintained through that counterparty. This risk applies in particular where client assets are held on an omnibus basis or where segregation is not fully recognised in the counterparty's jurisdiction.

5. Operational and information risks

Due to the irrevocability of blockchain transactions, incorrect approvals or the use of wrong networks or addresses will typically make the transferred funds irrecoverable. Because trading may also rely on technical connections to other venues or service providers, downtime or faulty code in these connections can temporarily block trading, deposits, or withdrawals even when the underlying blockchain is functioning. In addition, different groups of market participants may have unequal access to technical, governance, or project-related information, which can lead to information asymmetry and place less informed investors at a disadvantage when making trading decisions.

6. Market access and liquidity concentration risk

If the crypto-asset is only available on a limited number of trading platforms or through a single market-making entity, this may result in reduced liquidity, greater price volatility, or periods of inaccessibility for retail holders.

I.2 Issuer-related risks

Interpretative note for this section: Where no identifiable issuer exists, or where the crypto-asset project follows a decentralised structure, the risks described in this section should be read in light of that structure. References to the "issuer" do not constitute a determination that any foundation, development contributor, governance body, ecosystem participant, or other person is the issuer of the crypto-asset for the purposes of Regulation (EU) 2023/1114. Instead, the relevant risks may arise from the absence of a central responsible issuer or from the actions, omissions, financial condition, operational capacity, governance arrangements, communications, or continued involvement of persons or entities that may materially influence the development, operation, maintenance, or adoption of the crypto-asset.

1. Absence or insolvency of an identifiable issuer

Where an identifiable issuer exists, that issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, legal or regulatory developments, or external shocks, including pandemics or armed conflicts. In such a case, ongoing development, support, communication, or governance of the crypto-asset project may be reduced, suspended, or discontinued, potentially affecting the viability, availability, market acceptance, or tradability of the crypto-asset.

2. Legal and regulatory risks

The issuer operates in a dynamic and evolving regulatory environment. Failure to comply with applicable laws or regulations in relevant jurisdictions may result in enforcement actions, penalties, or restrictions on the project's operations. These may negatively impact the crypto-asset's availability, market acceptance, or legal status.

3. Operational risks

The issuer may fail to implement adequate internal controls, risk management, or governance processes. This can result in operational disruptions, financial losses, delays in updating the white paper, or reputational damage.

4. Governance and decision-making

The issuer's management body is responsible for key strategic, operational, and disclosure decisions. Ineffective governance, delays in decision-making, or lack of resources may compromise the stability of the project and its compliance with MiCA requirements. High concentration of decision-making authority or changes in ownership/control can amplify these risks.

5. Reputational risks

The issuer's reputation may be harmed by internal failures, external accusations, or association with illicit activity. Negative publicity can reduce trust in the issuer and impact the perceived legitimacy or value of the crypto-asset.

6. Counterparty dependence

The issuer may depend on third-party providers for certain core functions, such as technology development, marketing, legal advice, or infrastructure. If these partners discontinue their services, change ownership, or underperform, the issuer's ability to operate the project or maintain investor communication may be impaired. This could disrupt project continuity or undermine market confidence, ultimately affecting the crypto-asset's value.

I.3 Crypto-assets-related risks

1. Valuation risk

The crypto-asset does not represent a claim, nor is it backed by physical assets or legal entitlements. Its market value is driven solely by supply and demand dynamics and may fluctuate significantly. In the absence of fundamental value anchors, such assets can lose their entire market value within a very short time. Historical market behaviour has shown that some types of crypto-assets – such as meme coins or purely speculative tokens – have become worthless. Investors should be aware that this crypto-asset may lose all of its value.

2. Market volatility risk

Crypto-asset prices can fluctuate sharply due to changes in market sentiment, macroeconomic conditions, regulatory developments, or technology trends. Such volatility may result in rapid and significant losses. Holders should be prepared for the possibility of losing the full amount invested.

3. Liquidity and price-determination risk

Low trading volumes, fragmented trading across venues, or the absence of active market makers can restrict the ability to buy or sell the crypto-asset. In such situations, it is not guaranteed that an observable market price will exist at all times. Spreads may widen materially, and orders may only be executable under unfavourable conditions, which can make liquidation costly or temporarily impossible.

4. Asset security risk

Loss or theft of private keys, unauthorised access to wallets, or failures of custodial or exchange service providers can result in the irreversible loss of assets. Because blockchain transactions are final, recovery of funds after a compromise is generally impossible.

5. Fraud and scam risk

The pseudonymous and irreversible nature of blockchain transactions can attract fraudulent schemes. Typical forms include fake or unauthorised crypto-assets imitating established ones, phishing attempts, deceptive airdrops, or social-engineering attacks. Investors should exercise caution and verify the authenticity of counterparties and information sources.

6. Legal and regulatory reclassification risk

Legislative or regulatory changes in the European Union or in the Member State where the crypto-asset is admitted to trading may alter its legal classification, permitted uses, or tradability. In third countries, the crypto-asset may be treated as a financial instrument or security, which can restrict its offering, trading, or custody.

7. Absence of investor protection

The crypto-asset is not covered by investor-compensation or deposit-guarantee schemes. In the event of loss, fraud, or insolvency of a service provider, holders may have no access to recourse mechanisms typically available in regulated financial markets.

8. Counterparty risk

Reliance on third-party exchanges, custodians, or intermediaries exposes holders to operational failures, insolvency, or fraud of these parties. Investors should conduct due diligence on service providers, as their failure may lead to the partial or total loss of held assets.

9. Reputational risk

Negative publicity related to security incidents, misuse of blockchain technology, or associations with illicit activity can damage public confidence and reduce the crypto-asset's market value.

10. Community and sentiment risk

Because the crypto-asset's perceived relevance and expected future use depend largely on community engagement and the prevailing sentiment, a loss of public interest, negative coverage or reduced activity of key contributors can materially reduce market demand.

11. Macroeconomic and interest-rate risk

Fluctuations in interest rates, exchange rates, general market conditions, or overall market volatility can influence investor sentiment towards digital assets and affect the crypto-asset's market value.

12. Taxation risk

Tax treatment varies across jurisdictions. Holders are individually responsible for complying with all applicable tax laws, including the reporting and payment of taxes arising from the acquisition, holding, or disposal of the crypto-asset.

13. Anti-money-laundering and counter-terrorist-financing risk

Wallet addresses or transactions connected to the crypto-asset may be linked to sanctioned or illicit activity. Regulatory responses to such findings may include transfer restrictions, report obligations, or the freezing of assets on certain venues.

14. Market-abuse risk

Due to limited oversight and transparency, crypto-assets may be vulnerable to market-abuse practices such as spoofing, pump-and-dump schemes, or insider trading. Such activities can distort prices and expose holders to sudden losses.

15. Legal ownership and jurisdictional risk

Depending on the applicable law, holders of the crypto-asset may not have enforceable ownership rights or effective legal remedies in cases of disputes, fraud, or service failure. In certain jurisdictions, access to exchanges or interfaces may be restricted by regulatory measures, even if on-chain transfer remains technically possible.

16. Concentration risk

A large proportion of the total supply may be held by a small number of holders. This can enable market manipulation, governance dominance, or sudden large-scale liquidations that adversely affect market stability, price levels, and investor confidence.

I.4 Project implementation-related risks

As this white paper relates to the admission to trading of the crypto-asset, the following risk description reflects general implementation risks on the crypto-asset service provider's side typically

associated with crypto-asset projects. The party admitting the asset to trading is not involved in the project's implementation and does not assume responsibility for its governance, funding, or execution.

Delays, failures, or changes in the implementation of the project as outlined in its public roadmap or technical documentation may negatively impact the perceived credibility or usability of the crypto-asset. This includes risks related to project governance, resource allocation, technical delivery, and team continuity.

Key-person risk: The project may rely on a limited number of individuals for development, maintenance, or strategic direction. The departure, incapacity, or misalignment of these individuals may delay or derail the implementation.

Timeline and milestone risk: Project milestones may not be met as announced. Delays in feature releases, protocol upgrades, or external integrations can undermine market confidence and affect the adoption, use, or value of the crypto-asset.

Delivery risk: Even if implemented on time, certain functionalities or integrations may not perform as intended or may be scaled back during execution, limiting the token's practical utility.

I.5 Technology-related risks

As this white paper relates to the admission to trading of the crypto-asset, the following risks concern the underlying distributed ledger technology (DLT), its supporting infrastructure, and related technical dependencies. Failures or vulnerabilities in these systems may affect the availability, integrity, or transferability of the crypto-asset.

1. Blockchain dependency risk

The functionality of the crypto-asset depends on the continuous and stable operation of the blockchain(s) on which it is issued. Network congestion, outages, or protocol errors may temporarily or permanently disrupt on-chain transactions. Extended downtime or degradation in network performance can affect trading, settlement, or usability of the crypto-asset.

2. Smart contract vulnerability risk

The smart contract that defines the crypto-asset's parameters or governs its transfers may contain coding errors or security vulnerabilities. Exploitation of such weaknesses can result in unintended token minting, permanent loss of funds, or disruption of token functionality. Even after external audits, undetected vulnerabilities may persist due to the immutable nature of deployed code.

3. Wallet and key-management risk

The custody of crypto-assets relies on secure private key management. Loss, theft, or compromise of private keys results in irreversible loss of access. Custodians, trading venues, or wallet providers may be targeted by cyberattacks. Compatibility issues between wallet software and changes to the

blockchain protocol (e.g. network upgrades) can further limit user access or the ability to transfer the crypto-asset.

Outdated or vulnerable wallet software:

Users relying on outdated, unaudited, or unsupported wallet software may face compatibility issues, security vulnerabilities, or failures when interacting with the blockchain. Failure to update wallet software in line with protocol developments can result in transaction errors, loss of access, or exposure to known exploits.

4. Network security risks

Attack Risks: Blockchains may be subject to denial-of-service (DoS) attacks, 51% attacks, or other exploits targeting the consensus mechanism. These can delay transactions, compromise finality, or disrupt the accurate recording of transfers.

Centralisation Concerns: Despite claims of decentralisation, a relatively small number of validators or a high concentration of stake may increase the risk of collusion, censorship, or coordinated network downtime, which can affect the resilience and operational reliability of the crypto-asset.

5. Bridge and interoperability risk

Where tokens can be bridged or wrapped across multiple blockchains, vulnerabilities in bridge protocols, validator sets, or locking mechanisms may result in loss, duplication, or misrepresentation of assets. Exploits or technical failures in these systems can instantly impact circulating supply, ownership claims, or token fungibility across chains.

6. Forking and protocol-upgrade risk

Network upgrades or disagreements among node operators or validators can result in blockchain "forks", where the blockchain splits into two or more incompatible versions that continue separately from a shared past. This may lead to duplicate token representations or incompatibilities between exchanges and wallets. Until consensus stabilises, trading or transfers may be disrupted or misaligned. Such situations may be difficult for retail holders to navigate, particularly when trading platforms or wallets display inconsistent token information.

7. Economic-layer and abstraction risk

Mechanisms such as gas relayers, wrapped tokens, or synthetic representations may alter the transaction economics of the underlying token. Changes in transaction costs, token demand, or utility may reduce its usage and weaken both its economic function and perceived value within its ecosystem.

8. Spam and network-efficiency risk

High volumes of low-value ("dust") or automated transactions may congest the network, slow validation times, inflate ledger size, and raise transaction costs. This can impair performance, reduce throughput, and expose address patterns to analysis, thereby reducing network efficiency and privacy.

9. Front-end and access-interface risk

If users rely on centralised web interfaces or hosted wallets to interact with the blockchain, service outages, malicious compromises, or domain expiries affecting these interfaces may block access to the crypto-asset, even while the blockchain itself remains fully functional. Dependence on single web portals introduces a critical point of failure outside the DLT layer.

10. Decentralisation claim risk

While the technical infrastructure may appear distributed, the actual governance or economic control of the project may lie with a small set of actors. This disconnect between marketing claims and structural reality can lead to regulatory scrutiny, reputational damage, or legal uncertainty – especially if the project is presented as 'community-governed' without substantiation.

I.6 Mitigation measures

None.

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts

J.1 Adverse impacts on climate and other environment-related adverse impacts

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the crypto-asset

Aave Token

S.4 Consensus Mechanism

The crypto-asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Huobi Token, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR Protocol and Avalanche. In general, when evaluating crypto-assets, all implementations across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Ethereum:

Ethereum'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, and a validator is randomly selected to propose each new block. Once proposed, the other validators verify the block's integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalisation 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 behaviour or inactivity. PoS aims to improve energy efficiency, security, and scalability, with upgrades such as Proto-Danksharding (EIP-4844) already implemented to enhance Layer 2 scalability and transaction efficiency.

The following applies to Huobi:

Disclaimer: The HECO DAO has announced that the HECO Network (Huobi ECO Chain) will officially cease operations on January 15, 2025.

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

Key Features of HECO's Consensus Mechanism:

1. Validator Selection: HECO supports up to 21 validators, selected based on their stake in the network.

2. Transaction Processing: Validators are responsible for processing transactions and adding blocks to the blockchain.

3. Transaction Finality: The consensus mechanism ensures quick finality, allowing for rapid confirmation of transactions.

4. Energy Efficiency: By utilizing PoS elements, HECO reduces energy consumption compared to traditional Proof-of-Work systems.

The following applies to Gnosis Chain:

Gnosis operates with a Proof-of-Stake (PoS) consensus mechanism, where validators secure the network by staking GNO tokens and participating in block production.

The following applies to Polygon:

Polygon is a scaling solution for Ethereum that stores and process transaction data on its own separate chain and regularly submits checkpoints to Ethereum. This type of scaling solution is sometimes referred to as a plasma chain, and is distinct from sidechains, which don't store

checkpoints and Layer 2 solutions that store all transaction data on Ethereum in addition to the checkpoints. 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 POL tokens they have staked. The more tokens are 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 POL tokens to validators. Delegated tokens also count towards the block production chance of the validator they are delegated to. Delegators receive a share of rewards earned by validators.

Consensus Process

2. Transaction Validation: Transactions are first validated by validators who have staked POL tokens. These validators confirm the validity of transactions and include them in blocks.

3. Block Production: Proposing and Voting: Validators are randomly selected to propose new blocks. Their selection chance is proportional to their staked tokens. Validators also participate in a voting process to reach consensus on the next block. The block with most votes is added to the blockchain. Checkpointing: Polygon uses periodic checkpointing, where a cryptographic summary of the transactions on the Polygon chain is submitted to the Ethereum main chain. This process ensures the security and finality of transactions on the Polygon network.

The following applies to Binance Smart Chain:

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 decentralisation 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 decentralisation 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, incentivising 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 decentralisation.

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 behaviour. This staked amount can be slashed if validators act maliciously. Staking incentivises 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 incentivises 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 incentivising them to validate transactions accurately and efficiently.

The following applies to Solana:

Solana uses a combination of Proof-of-History (PoH) and Proof-of-Stake (PoS). The core concepts of the mechanism are intended to work as follows:

Core Concepts

1. Proof-of-History (PoH):

PoH is a cryptographic ordering and timing mechanism that provides evidence that data existed in a particular sequence and that time passed between proofs.

Verifiable Delay Function (VDF): PoH relies on a sequential hash-based proof process that Solana describes as VDF-like. 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: Leader slots are assigned through the network's leader schedule, which is stake-weighted. The more SOL 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 contributing to the network's security.

Consensus Process

1. Transaction Validation:

Transactions are broadcasted 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 Finalisation:

Other validators vote on the ledger state associated with the block. A block may first become confirmed and later finalised once it reaches the network's strongest confirmation state.

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: Staking provides economic alignment, and Solana documentation notes that slashing has been discussed as a future mechanism for intentional malicious behaviour, but is not implemented yet.

Delegated Staking: Token holders can delegate their SOL tokens to validators, intended to enhance network security and decentralisation. Delegators share in the rewards and are incentivised to choose reliable validators.

3. Economic Penalties:

Slashing (planned): Validators can be penalized for malicious behaviour, 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.

The following applies to NEAR Protocol:

1. Core consensus model

- NEAR does not use miners; instead, it relies on validators that stake NEAR tokens to participate in block and chunk production.

- Nightshade is a sharded consensus model in which all shards jointly produce a single logical block for each block height.

- Each shard produces a chunk containing transactions and state changes for that shard, and a designated block producer aggregates all chunks into one block.

2. Validator roles

- Block and Chunk Producers are responsible for creating blocks and producing shard chunks.

- Chunk Validators verify the correctness of chunks produced by other validators.

- Hidden Validators are randomly assigned to shards using a Verifiable Random Function (VRF) and verify chunk correctness without their assignment being known in advance.

- Fishermen are observing nodes that monitor the network and can submit fraud proofs if invalid behaviour is detected.

3. Block production and finality

- Blocks and chunks are produced at an interval of approximately one second.

- Transactions become final once all related receipts (cross-shard execution messages) have been processed.

- Most transactions reach finality within 1 to 3 seconds, depending on cross-shard execution.

The following applies to Avalanche:

The Avalanche C-Chain uses the Snowman++ consensus mechanism, which is Avalanche's consensus model for linear blockchains and is implemented through the ProposerVM wrapper. Under this model, validators repeatedly query a small random subset of other validators and converge on a preferred block once the required confidence thresholds are met. Avalanche documentation describes the baseline Snowman parameters with a sample size of k = 20, quorum threshold α = 14, and decision threshold β = 20, while also noting that the AvalancheGo implementation includes additional optimisations for latency and throughput.

Only Primary Network validators are entitled to validate the C-Chain. To participate as a validator on Avalanche mainnet, a node must stake a minimum of 2,000 AVAX for a period of 14 to 365 days. Token holders may also participate indirectly by delegating at least 25 AVAX to an existing validator. Validator identity and admission to staking require the relevant staking credentials, including BLS proofs of possession under the current staking framework.

For block production, Snowman++ uses stake-weighted proposer windows. Through the ProposerVM, block-building opportunities are assigned to proposers in 5-second windows, after which block production may fall back more broadly to validators if necessary. This mechanism is intended to regulate block production while preserving network liveness. Consensus voting itself remains based on repeated sub-sampled polling rather than fixed validator committees.

Avalanche documentation describes the finality model as sub-second and treated by the protocol as final and irreversible once accepted, while noting that safety is probabilistic in the formal sense because the probability of conflicting acceptance can be reduced to an arbitrarily low level through the protocol parameters. The protocol does not rely on slashing of staked principal. Instead, validator reward eligibility depends on compliance with protocol conditions, including uptime requirements. Under current Avalanche documentation, the validator uptime threshold for reward eligibility is 90%, following ACP-267.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Huobi Token, Gnosis Chain, Polygon, Binance Smart Chain, Solana, NEAR

Protocol and Avalanche. In general, when evaluating crypto-assets, all implementations across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Ethereum:

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.

The following applies to Huobi:

Disclaimer: The HECO DAO has announced that the HECO Network (Huobi ECO Chain) will officially cease operations on January 15, 2025.

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.

The following applies to Gnosis Chain:

Validators on Gnosis earn GNO rewards for validating transactions and securing the network. Transaction fees are used to compensate for network resources and maintain stability.

The following applies to Polygon:

Incentive Mechanisms

1. Validators: Staking Rewards: Validators on Polygon secure the network by staking POL tokens. Validators are rewarded for block production and block validation/voting. They earn rewards in the form of newly minted POL tokens and, when they produce blocks, some transaction fees.

2. Delegators: Delegation: Token holders who do not wish to run a validator node can delegate their POL tokens to trusted validators. Delegators earn a portion of the rewards earned by the validators, incentivising them to choose reliable and performant validators. Validators profit from delegations, because their chance of being selected for block production and therefore the associated expected rewards increase. This system encourages widespread participation and enhances the network's decentralisation.

3. Economic Security: Slashing: Validators can be penalised through a process called slashing if they engage in malicious behaviour 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 POL tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity.

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

The following applies to Binance Smart Chain:

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivise 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 incentivises token holders to participate in the network’s security and decentralisation 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 penalised for malicious behaviour 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

5. 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.

6. Block Rewards: Incentivising 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.

7. 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.

8. Smart Contract Fees: Deployment and Execution Costs: 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 following applies to Solana:

1. Validators:

Validators participate in block production and voting under Solana's stake-weighted model. They may receive staking-related rewards and a share of transaction-fee income. Under Solana's fee model, the base fee is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This is intended to provide 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 the rewards earned by the validators. This is intended to encourage widespread participation in securing the network and to support decentralisation.

3. Economic Security:

Solana staking documentation notes slashing as a possible future mechanism for intentional malicious conduct, but states that slashing is not implemented in the protocol today. Economic alignment instead currently arises primarily from staking participation, validator performance incentives, and the opportunity cost of locking capital in staking positions.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana transactions require fees in SOL. The fee model consists of a base fee and, where used, an optional prioritisation fee. The base fee compensates signature verification work and is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

2. Rent Fees:

Solana accounts that store on-chain state must satisfy the rent-exemption threshold, which is linked to the amount of data stored. This mechanism is intended to support efficient use of network state and account storage resources.

3. Program Execution Costs:

Deploying and interacting with on-chain programs may involve transaction fees and, where relevant, compute-related prioritisation fees and account-storage requirements. These mechanisms are intended to allocate network resources in proportion to use.

The following applies to NEAR Protocol:

1. Validator incentives

- Validators must stake NEAR tokens in order to participate in block and chunk production.

- Validators receive epoch rewards every epoch (approximately 12 hours, or 43,200 blocks).

- The protocol targets an annual validator reward rate of approximately 2.5% to 4.5% of the total token supply, depending on how much NEAR is staked across the network.

- Rewards are socialized, meaning validators are paid based on their stake rather than the number of transactions or shards they directly process.

- Maximum annual protocol inflation is capped at 5%, of which 4.5% is used for validator rewards and 0.5% is allocated to the Protocol Treasury.

2. Transaction fees and fee burning

- Transaction fees on NEAR are paid in NEAR tokens.

- 100% of gas fees (after the developer rebate) are burned, permanently removing those tokens from circulation.

- 30% of the gas fees generated by a smart-contract call are automatically paid to the contract account as a developer rebate.

- Fee burning offsets inflation and may make the token supply deflationary during periods of high network usage.

3. Developer incentives

- Developers earn 30% of the gas fees generated when users interact with their smart contracts.

- These rewards are paid directly and automatically by the protocol, allowing developers to monetize applications without issuing their own tokens.

4. Storage staking incentives

- Users and developers must stake NEAR tokens to store data on-chain.

- The storage cost is approximately 1 NEAR per 100 kB of state.

- Tokens locked for storage cannot be used for validation staking, reducing the total circulating supply and indirectly increasing validator yields.

5. Slashing and economic penalties

- Validators risk losing their staked NEAR if they misbehave.

- Double signing results in progressive slashing, up to the full stake if a large portion of validators misbehave.

- Producing an invalid chunk results in 100% slashing of the validator's stake.

- Validators that confirm erasure-coded land mines are immediately slashed.

- Validators that fail to meet production requirements can be removed from the active set through kickout thresholds.

6. Fishermen and protocol treasury

- Fishermen monitor the network and submit fraud proofs. They must post a 10 NEAR bond, which is lost if they submit false challenges.

- 10% of protocol inflation (approximately 0.5% of total supply per year) is allocated to a Protocol Treasury used to fund ecosystem development, infrastructure and education.

The following applies to Avalanche:

The Avalanche C-Chain is secured economically through the native AVAX token. Validator incentives are based primarily on staking rewards, not on redistribution of C-Chain transaction fees. A fixed amount of 360 million AVAX was minted at genesis, while additional AVAX is minted over time as validator rewards, subject to Avalanche's capped token supply framework. Validator rewards are paid at the end of the staking period and are determined by factors such as the validator's stake and compliance with staking conditions.

Unlike some proof-of-stake systems, the Avalanche Primary Network does not use slashing of bonded principal as an ordinary penalty mechanism. Instead, the main protocol-level economic consequence for underperformance is the loss of reward eligibility. Where a validator fails to satisfy the applicable uptime requirement during its staking term, that validator does not receive the corresponding staking reward. In current Avalanche documentation, the required uptime level for reward eligibility is 90%.

Transaction fees apply on the C-Chain for transfers and smart-contract execution. The fee model follows EIP-1559 logic, meaning that transactions are priced through a dynamic base fee mechanism. In contrast to Ethereum's validator tip model, C-Chain transaction fees are burned rather than distributed to validators. This means that C-Chain fees function as a supply-reduction mechanism and are intended in part to offset inflation arising from the minting of validator rewards.

In addition to ordinary transaction and smart-contract execution fees, Avalanche documentation also recognises protocol fees in connection with other network operations on other chains of the Primary Network, such as certain import or export operations and staking-related actions. However, for the C-Chain itself, the core applicable fee category is the gas fee for transaction inclusion and contract execution, and those fees are handled through the protocol burn mechanism rather than paid to validators or a treasury.

S.6 Beginning of the period to which the disclosure relates

2025-02-12

S.7 End of the period to which the disclosure relates

2026-02-12

S.8 Energy consumption

7392.01120 kWh/a

S.9 Energy consumption sources and methodologies

The energy consumption associated with this crypto-asset is aggregated of multiple contributing components, primarily the underlying blockchain network and the execution of token-specific operations. To determine the energy consumption of a token, the energy consumption of the underlying blockchain network : Avalanche, Binance Smart Chain, Ethereum, Gnosis Chain, Huobi, Near Protocol, Polygon, Solana is calculated first. A proportionate share of that energy use is then attributed to the token based on its activity level within the network (e.g. transaction volume, contract execution).

The Functionally Fungible Group Digital Token Identifier (FFG DTI) is used to determine all technically equivalent implementations of the crypto-asset in scope.

Estimates regarding hardware types, node distribution, and the number of network participants are based on informed assumptions, supported by best-effort verification against available empirical data. Unless robust evidence suggests otherwise, participants are assumed to act in an economically rational manner. In line with the precautionary principle, conservative estimates are applied where uncertainty exists – that is, estimates tend towards the higher end of potential environmental impact.

S.10 Renewable energy consumption

37.5413907826 %

S.11 Energy intensity

0.00004 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

2.46016 tCO2e/a

S.14 GHG intensity

0.00001 kgCO2e

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 incentivisation 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 incentivisation 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 licensed under CC BY 4.0.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.