CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG ZN1MJGVLX

Preamble

00. Table of Contents

01. Date of notification

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

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 AXL referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed on the Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom (legacy; scheduled for retirement on 30 June 2026) and Avalanche C-Chain networks according to the DTI FFG shown in section F.14, as of 2026-04-28. The maximum supply of the crypto-asset is unlimited. As of the launch of the Axelar Network token in September 2022, an initial supply of 1,000,000,000 AXL was created and distributed among key stakeholders. As of the time of writing of this white paper, the total supply is approximately 1,239,524,722 AXL, with current yearly inflation of approximately 3.8%. The first network activity on Axelar can be viewed on 2021-12-22 (block hash: B31837704EA4C6470B89929638F19DB12BAD1CA5416E7D3247E814091264542C, source: https://www.mintscan.io/axelar/block/1, accessed 2026-04-28). The network token AXL was launched in September 2022. The first network activity on Ethereum can be viewed on 2022-08-29 (transaction hash: 0xf5d0a60c56f3666d7b15ff9bdea8570efe6aa5616009f4cc2e3730799bfb97e7, source: https://etherscan.io/tx/0xf5d0a60c56f3666d7b15ff9bdea8570efe6aa5616009f4cc2e3730799bfb97e7, accessed 2026-04-28). The first network activity on Osmosis can be viewed on 2022-03-07 (channel: OSMOSIS/channel-208, source: https://www.mintscan.io/osmosis/relayers/channel-208/axelar/channel-3, accessed 2026-04-28). The first network activity on Linea can be viewed on 2023-07-21 (transaction hash: 0x2732d4e60ff379f69ae44672404d1bd9bceda5d87404348121ab91174816c150, source: https://lineascan.build/tx/0x2732d4e60ff379f69ae44672404d1bd9bceda5d87404348121ab91174816c150, accessed 2026-04-28). The first network activity on Mantle can be viewed on 2023-08-31 (transaction hash: 0xaeb95025cfa8bfe60c27a4835dea77ae1659e7da7500e162db0834276f2678e9, source: https://mantlescan.xyz/tx/0xaeb95025cfa8bfe60c27a4835dea77ae1659e7da7500e162db0834276f2678e9, accessed 2026-04-28). The first network activity on Arbitrum can be viewed on 2022-12-05 (transaction hash: 0x7835258777b1b841dd0d403c842c21281a37e1a3b0b42b4a379f8418e6cd7a58, source: https://arbiscan.io/tx/0x7835258777b1b841dd0d403c842c21281a37e1a3b0b42b4a379f8418e6cd7a58, accessed 2026-04-28). The first network activity on BNB Chain can be viewed on 2022-08-29 (transaction hash: 0x8a970c18b7cd45c61a4f2b2df1fb28d2973bf7b4e2a5b84932ed7452e537a287, source: https://bscscan.com/tx/0x8a970c18b7cd45c61a4f2b2df1fb28d2973bf7b4e2a5b84932ed7452e537a287, accessed 2026-04-28). The first network activity on Base can be viewed on 2023-07-21 (transaction hash: 0x6f484b5a40fa2ea50bc2edfc602a4f159973cc9f82911f9e7ced7f773a76d601, source: https://basescan.org/tx/0x6f484b5a40fa2ea50bc2edfc602a4f159973cc9f82911f9e7ced7f773a76d601, accessed 2026-04-28). The first network activity on Polygon can be viewed on 2022-08-29 (transaction hash: 0x194e0a4add5656e7e0f744ae17a3ce25d07da74d3a77b32fcbf96e81650abedf, source: https://polygonscan.com/tx/0x194e0a4add5656e7e0f744ae17a3ce25d07da74d3a77b32fcbf96e81650abedf, accessed 2026-04-28). The first network activity on Optimism can be viewed on 2023-06-09 (transaction hash: 0x2310b12e74e12952e520e0b3b84b6d9e589c0c632c2f68f1728c1ebafb5ce6e1, source: https://optimistic.etherscan.io/tx/0x2310b12e74e12952e520e0b3b84b6d9e589c0c632c2f68f1728c1ebafb5ce6e1, accessed 2026-04-28). The first network activity on Fantom can be viewed on 2022-08-29 (transaction hash: 0xeac894715adb9ec27d220aa1e58d2809607b672eda10374be5e076e0efb27aa8, source: https://www.oklink.com/fantom/tx/0xeac894715adb9ec27d220aa1e58d2809607b672eda10374be5e076e0efb27aa8, accessed 2026-04-28). Since the migration of Fantom (FTM) to Sonic (S) was completed on 10 May 2025, the Fantom network should be understood as legacy infrastructure. The first network activity on Avalanche C-Chain can be viewed on 2022-08-29 (transaction hash: 0xe8120b5e36207a68ad188a22453f188f68d465ba486ef3ba7c471b3b10178d1f, source: https://

avascan.info/blockchain/c/tx/ 0xe8120b5e36207a68ad188a22453f188f68d465ba486ef3ba7c471b3b10178d1f, accessed 2026-04-28).

The Axelar network is a decentralised interoperability platform designed to support communication between different blockchain networks, applications and users. The network enables cross-chain message passing and asset-related interactions through a validator network, gateway contracts deployed on connected networks, and development tools for programmable interchain functionality. The network uses a proof-of-stake consensus model for validator participation and verification of cross-chain events, while gateway contracts operate as technical entry and exit points for messages between connected networks. The project also includes the Axelar Virtual Machine, Interchain Token Service and related development tools that may be used by developers to build and operate applications across multiple blockchain environments.

The crypto-asset is used as the native token of the Axelar network. It is required for validator staking and is used in the network's proof-of-stake consensus process, with validator voting power linked to the amount of AXL staked. The crypto-asset may be used for network incentives, including rewards for validators and verifiers supporting the operation and security of connected network routes. It may also be used for on-chain governance, including voting on network upgrades, parameter changes and support for additional connected networks. AXL is also used in relation to network fees, and following the Cobalt upgrade a portion of collected gas fees is sent to a burn address, with the remaining portion directed to a community grant pool. Reward pools for newly connected blockchains may also be funded using AXL from the existing supply.

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 a 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 the 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,

DE-HH

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

Axelar Foundation

B.3 Legal form

The legal form of Axelar Foundation is K575, which corresponds to "Foundation company".

B.4 Registered address

The registered address of Axelar Foundation is Box 10176, Governor's Square, 23 Lime Tree Bay Ave., KY1-1002 George Town,

Cayman Islands,

KY1

B.5 Head office

Could not be found while drafting this white paper.

Could not be found while drafting this white paper.

Could not be found while drafting this white paper.

B.6 Registration date

The exact date of registration of the Axelar Foundation could not be determined based on publicly available information. However, available sources indicate that the foundation was registered in 2021.

B.7 Legal entity identifier

Axelar Foundation has no Legal Entity Identifier (LEI).

B.8 Another identifier required pursuant to applicable national law

Could not be found.

B.9 Parent company

No parent company of the Axelar Foundation can be identified.

B.10 Members of the management body

Identity	Function	Business Address
Georgios Vlachos	Director	Box 10176, Governor's Square, 23 Lime Tree Bay Ave., KY1-1002 George Town, Cayman Islands
Nikolaos Rapanos	Director	Box 10176, Governor's Square, 23 Lime Tree Bay Ave., KY1-1002 George Town, Cayman Islands

B.11 Business activity

Axelar Foundation is a non-profit established to support the growth and adoption of the Axelar network, a decentralised interoperability platform that serves multiple blockchain ecosystems.

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 since Crypto Risk Metrics GmbH is not a trading platform.

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-Asset white paper Preparation

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

C.10 Members of the Management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

Not applicable since 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 since 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 since 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: "Axelar", Short Name: "AXL" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-30).

D.2 Crypto-assets name

Long Name: "Axelar" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-30).

D.3 Abbreviation

Short Name: "AXL" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-30).

D.4 Crypto-asset project description

According to public information published in the Axelar documentation and related project resources (sources: https://www.axelar.network/blog, https://docs.axelar.dev/; accessed 2026-04-28), the Axelar project is a decentralised interoperability network designed to support cross-chain communication between distinct blockchain ecosystems. The project focuses on enabling the transmission of messages, execution of smart-contract logic, and transfer of digital assets across multiple distributed ledger networks within a unified technical framework. Its architecture includes a Proof-of-Stake based blockchain built using the Cosmos SDK, a decentralised validator set responsible for network security and message verification, and supporting components such as Gateways deployed on connected chains, relayer infrastructure, and generalised cross-chain communication protocols.

The protocol incorporates mechanisms such as General Message Passing, which enables the execution of arbitrary function calls across supported networks, and an Interchain Token Service, which facilitates the issuance and management of tokens across multiple chains while maintaining functional consistency. The system also includes multiparty cryptographic schemes for the management of cross-chain authorisation processes, as well as operational components for fee abstraction and transaction coordination. The protocol supports ongoing technical development relating to interoperability, validator participation, cross-chain security, and application deployment across an expanding set of connected blockchain environments.

The AXL crypto-asset functions as a core technical element within this broader framework. It is used in connection with network security through staking mechanisms, validator participation, and governance-related processes, and may also be used in relation to transaction fee handling and protocol-level operations. The crypto-asset operates as part of the technical infrastructure supporting cross-chain communication and coordination within the Axelar network.

The project does not involve the granting of ownership, profit-participation rights, or legal claims against the Axelar protocol or its contributors. Instead, it centres on the creation of a technical environment in which the AXL crypto-asset may serve as an operational input for certain protocol processes. The long-term evolution of the Axelar system, including the scope of available features, the validator-participation framework, committee- or leader-selection mechanisms, 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
Axelar Foundation	Other person involved in implementation	Box 10176, Governor's Square, 23 Lime Tree Bay Ave., KY1-1002 George Town, Cayman Islands	Cayman Islands
Georgios Vlachos	Other person involved in implementation	Box 10176, Governor's Square, 23 Lime Tree Bay Ave., KY1-1002 George Town, Cayman Islands	Cayman Islands
Nikolaos Rapanos	Other person involved in implementation	Box 10176, Governor's Square, 23 Lime Tree Bay Ave., KY1-1002 George Town, Cayman Islands	Cayman Islands
Sergey Gorbunov	Other person involved in implementation	1824 Store St. 2nd Floor Victoria BC V8T 4R4 Canada	Canada
Interop Labs Inc.	Other person involved in implementation	1824 Store St. 2nd Floor Victoria BC V8T 4R4 Canada	Canada

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 a 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 a service supplied solely by the issuer.

D.8 Plans for the token

This section provides an overview of the historical developments related to the AXL 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 was a formally published roadmap for the AXL crypto-asset and the Axelar protocol covering prior development periods, including 2024 and 2025. Based on the official roadmap and public sources (sources: https://www.axelar.network/blog, https://docs.axelar.dev/; accessed 2026-04-28), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Axelar protocol and the role of the AXL crypto-asset.

Past milestones:

- Initial White Paper Release (January 2021): The first draft (version 1.0) of the Axelar white paper was published.

- Mainnet Launch (February 2022): The Axelar mainnet became operational.

- General Message Passing Deployment (May 2022): The GMP protocol was implemented on the mainnet, enabling cross-chain communication.

- Token Release and Governance Update (September 2022): Quadratic voting was introduced and the AXL crypto-asset was released on the mainnet.

- Network Expansion Milestone (October 2023): The protocol reached connectivity with 50 blockchains.

- Axelar Virtual Machine Deployment (March 2024): The AVM was introduced following governance approval.

- Cobalt Upgrade (25 February 2025): Version 1.2.1 was implemented, modifying tokenomics by directing a substantial share of gas fees to a burn mechanism.

Future milestones:

- Additional Network Integrations (Ongoing): Further integrations with networks are anticipated as part of the Interchain Amplifier framework.

- Long-term Ecosystem Expansion (Long-term): The project anticipates positioning the protocol to support broader adoption trends in digital finance, including large-scale shifts in asset ownership structures.

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 AXL 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 AXL token has conducted multiple funding rounds involving seed financing, venture capital investment, and strategic participation from institutional and angel investors.

According to publicly referenced information, on or around 12 November 2020, the project is reported to have completed a seed funding round in the amount of approximately USD 3,750,000. This round was led by Binance X, the Binance Smart Chain Accelerator Fund, and DCVC (Data Collective), with additional participation from Lemniscap, Collab+Currency, North Island Ventures, Divergence Ventures, Cygni Labs, Waikit Lau, and Naval Ravikant.

Public sources further indicate that, in or around mid-2021, the project completed a Series A funding round in the amount of approximately USD 25,000,000, led by Polychain Capital. Additional participants in this round are reported to include Dragonfly Capital, Galaxy Digital, North Island Ventures, Robot Ventures, Collab+Currency, Cygni Capital, Lemniscap, Divergence Ventures, SCB 10X, Hypersphere, Zola Global Investors, Morningstar Ventures, Nima Capital, and GoldenCoin TS LLC. Third-party reporting also references participation from individual angel investors, including Do Kwon, Happy Walters, and Waikit Lau.

Further public reporting indicates that, on or around 15 February 2022, the project completed a Series B funding round in the amount of approximately USD 35,000,000. This round is reported to have included participation from Dragonfly Capital, Polychain Capital, North Island Ventures, Rockaway Blockchain Fund, Cygni Capital, Lemniscap, Olive Tree Capital, Blockchange Ventures, and Node Capital, alongside angel investors such as Waikit Lau and Gokul Rajaram. Public sources further indicate that this round implied a project valuation of approximately USD 1,000,000,000.

Publicly available information indicates that a public community token sale was conducted in or around March 2022. The sale was reportedly conducted at a token price of USD 1.00 per AXL. The announced allocation for the sale was 5% of the initial token supply, corresponding to 50,000,000 AXL, which would imply a maximum potential gross sale amount of USD 50,000,000 if fully sold. Publicly available information separately refers to an allocated supply of 28,600,000 AXL, corresponding to approximately USD 28,600,000 at the stated sale price. Public sources do not consistently confirm the final gross proceeds actually received from the sale.

However, all such information is derived exclusively from public announcements, portfolio disclosures, press releases, transparency reports, and third-party publications. The issuer, foundation, or entities associated with the AXL crypto-asset have not independently confirmed the occurrence, precise amounts, valuation, legal structure, or contractual terms of these reported financing rounds. As a result, the referenced investment amounts, investor participation, and any implied 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

As of 4 May 2026, the total supply of AXL was approximately 1,239,524,722 AXL. AXL does not have a fixed maximum supply. At the genesis block, 1,000,000,000 AXL were created and allocated across several stakeholder groups, including community programmes, backers, team members, community operations and a community sale. The supply of AXL may change over time through protocol-defined mechanisms, including inflationary rewards for network participants and token burning mechanisms relating to network fees. Publicly available information indicates that recent tokenomics changes introduced a fee-burning mechanism intended to offset part of the inflationary issuance. As a result, the total supply of AXL may increase over time, while the effective circulating supply may also be reduced by burns. Investors should note that changes in the effective supply, including increases through issuance, releases of allocated tokens or reductions through burning, may affect the token's price and liquidity. The circulating supply may therefore 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 any additional restrictions that 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 transaction 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 crypto-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 it is not subject to any stabilisation mechanism. It is neither pegged to any fiat currency nor backed by any external assets, which distinguishes 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, and therefore remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

According to publicly available information in official Axelar documentation and related public sources (sources: https://www.axelar.network/blog, https://docs.axelar.dev/; accessed 2026-04-28), AXL is the native crypto-asset of the Axelar network and is intended to function as a core on-chain technical component within the Axelar protocol environment. AXL is used at protocol level for the processing of transaction fees associated with cross-chain communication, the coordination of validator activity, and participation in the network's proof-of-stake security model through staking and delegation. Documentation further indicates that validator participation and consensus

processes rely on the staking of AXL, with voting power linked to the amount of AXL delegated, and that protocol-level rewards may be distributed to validators and delegators in accordance with network rules. In addition, public information states that AXL may be used within governance processes, including the submission and voting on proposals relating to protocol parameters, network upgrades, and ecosystem development. Certain mechanisms described in public sources also include the conversion of transaction-related fees into AXL for protocol-level settlement and the burning of a portion of network fees under defined conditions.

The AXL crypto-asset 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 Axelar protocol environment. The usability of AXL depends on factors such as the continued operation of the relevant protocol infrastructure, the performance and security of the Axelar network, the correct functioning of consensus and cross-chain communication mechanisms, and future development decisions associated with the Axelar project.

F.3 Planned application of functionalities

Future milestones:

- Additional Network Integrations (Ongoing): Further integrations with networks are anticipated as part of the Interchain Amplifier framework.

- Long-term Ecosystem Expansion (Long-term): The project anticipates positioning the protocol to support broader adoption trends in digital finance, including large-scale shifts in asset ownership structures.

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 AXL 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 NEWT, which stands for "New".

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, and is available on the Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon, Optimism, Fantom and Avalanche C-Chain networks. The crypto-asset is fungible up to 6 digits after the decimal point. 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. These 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: "Axelar" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-30).

F.8 Website of the issuer

https://www.axelar.foundation/

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

2026-06-08

F.10 Publication date

2026-06-08

F.11 Any other services provided by the issuer

No such services are currently known to be provided by the issuer. However, 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

WWMN8KJWC, 6VGJMR9PK, 7XNZ3KK67, 9VSMXTSM2, D4W32DPGP, HPVXGTF8V, MVCDDN6Q2, PZ5PWDTV1, Q2QDNVB1X, TD3VWXG02, WF9C3FK6M, X5B92NG0R

F.14 Functionally fungible group digital token identifier

ZN1MJGVLX

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

The issuer is eligible for a Legal Entity Identifier (LEI).

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 legally enforceable claim against the issuer of the crypto-asset or any third party.

G.2 Exercise of rights and obligations

As the crypto-asset does not confer 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 project's technical infrastructure – such as participation mechanisms or protocol-level features – serves operational purposes only and does not create, evidence, or constitute 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 for modifying such rights or obligations. 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 rights exist and no rights arise under applicable law or regulation. Holders should not interpret technical updates or governance-related changes as amendments to legally binding entitlements.

G.4 Future public offers

Information on future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-04-28).

G.5 Issuer retained crypto-assets

At the genesis of the Axelar network, a total of 1,000,000,000 AXL tokens were created and allocated across multiple categories. According to publicly available information (source: https://medium.com/@axelar-foundation/axl-tokenomics-2-0-scaling-axelar-to-thousands-of-blockchains-4c4b921cb75a, accessed 2026-04-28), approximately 36% of the genesis supply was allocated to community programmes within the Axelar ecosystem, corresponding to approximately 360,000,000 AXL.

These community programme allocations are described as being managed within the ecosystem framework, including by the Axelar Foundation. However, publicly available information does not specify the exact number of AXL tokens currently retained directly by the Axelar Foundation or any other identifiable issuer entity.

Note: Although a portion of the genesis allocation is associated with ecosystem programmes, this does not necessarily imply direct or continuous ownership or control of such tokens by the Axelar Foundation. Token distributions, vesting schedules, treasury operations, or other reallocations may have occurred since the initial genesis allocation in September 2022. As a result, the current concentration and ownership of AXL tokens may differ from the initial allocation, and on-chain wallet addresses cannot be conclusively attributed to specific legal or natural persons.

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 2026-04-28.

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

Not applicable.

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 be brought before 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 Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is implemented on Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

The following applies to Axelar:

1. Network protocols

The Axelar network operates as a blockchain built using the Cosmos SDK and designed to provide cross-chain communication between independent blockchain networks. Consensus and peer-to-peer networking are provided by CometBFT, formerly Tendermint Core, which implements a Byzantine Fault Tolerant Proof-of-Stake consensus mechanism under which validators propose and vote on blocks to achieve finality. Communication between the consensus layer and the application layer is handled through the Application BlockChain Interface.

In addition to its base blockchain architecture, Axelar uses a cross-chain protocol suite designed to route, verify, and execute messages between heterogeneous blockchain ecosystems. The Cross-Chain Gateway Protocol functions as the routing layer for cross-chain communication and is used to connect independent blockchain networks to the Axelar network. The Cross-Chain Transfer Protocol operates as an application-level protocol on top of this routing layer and supports cross-chain requests, including the transfer of assets and the execution of cross-chain messages.

2. Cross-chain communication and transaction standards

Transactions on the Axelar network are defined at the application level and validated through a standardised processing pipeline that includes signature verification, sequence checks, gas accounting, and fee deduction. Accounts store authentication information such as public keys, addresses, balances, and sequence numbers, with addresses represented using formats compatible with Cosmos SDK-based chains.

Cross-chain transactions commonly begin when a user or decentralised application interacts with a gateway contract or gateway application on a connected source chain. Relayer services observe relevant events on the source chain and submit them to the Axelar network for validation. Axelar validators independently verify cross-chain events, including by querying nodes or RPC endpoints for connected external chains. Once a message or command has been validated, the network authorises execution on the destination chain through cryptographic signature processes and relayer submission.

3. Cryptographic standards and cross-chain authorisation

Axelar uses standard cryptographic primitives for transaction authentication, validator voting, and cross-chain authorisation. These include public-key cryptography, digital signature schemes such as ECDSA and Ed25519, hashing of messages and payloads, and Merkle-based verification methods.

For cross-chain execution, Axelar uses threshold signature schemes. Under this model, gateway signing authority is distributed across validators through cryptographic key shares rather than held by a single participant. A cross-chain command is authorised only when the required threshold of validator voting power participates in the signature process. This structure is intended to reduce reliance on any single validator or operator for the authorisation of cross-chain actions.

4. Blockchain data structure and block standards

The Axelar blockchain separates consensus from state execution in the same manner as other Cosmos SDK-based networks. CometBFT is responsible for block ordering and validator voting, while the application layer is responsible for deterministic state transitions. Application state is maintained using Merkle-based data structures and committed to each block through a cryptographic application hash.

Blocks contain ordered transactions and application-level messages, including messages relating to staking, governance, transfers, validator operations, and cross-chain event validation. Once a block obtains the required validator pre-commit threshold, it is finalised under the CometBFT consensus rules.

5. Upgrade and improvement standards

Protocol changes and network upgrades on Axelar may be coordinated through on-chain governance and scheduled software upgrade mechanisms. Governance proposals may address software upgrades, parameter changes, community pool spending, and other network-level decisions. Where a software upgrade is approved, validators are expected to run the updated software at the scheduled upgrade height in order to continue participating in consensus.

Axelar governance may also be used in connection with cross-chain functionality, including decisions concerning supported chains, supported assets, network parameters, and funding arrangements for network development or cross-chain security mechanisms.

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 Osmosis:

Osmosis is built on the Cosmos SDK and uses the Inter-Blockchain Communication (IBC) protocol for interoperability. These standards enable cross-chain interaction within the Cosmos ecosystem but remain dependent on the adoption and stability of the Cosmos framework. Reliance on a still-developing interoperability standard may introduce integration and security risks.

The following applies to Linea:

Linea uses rollup technology, whereby multiple transactions are aggregated ("rolled up") and submitted in batches to Ethereum for final settlement.

A sequencer is responsible for ordering transactions on the Linea network. The sequencer collects user-submitted transactions, orders them, and produces Linea blocks.

The correctness of Linea state transitions is ensured through a zero-knowledge prover mechanism. The prover generates cryptographic validity proofs demonstrating that the state transitions executed off-chain are consistent with the Ethereum smart contracts governing the rollup. These proofs are submitted to Ethereum, where a verifier contract confirms their validity prior to finalisation, ensuring that incorrect state transitions cannot be accepted on the base layer.

Linea is interoperable with Ethereum. Users deposit and withdraw assets via Ethereum smart contracts, and Linea transactions ultimately derive their security from Ethereum's consensus mechanism. Future upgrades may extend interoperability to other Layer 2 solutions or blockchains.

The following applies to Mantle:

Mantle is built upon Ethereum Layer 2 standards using an Optimistic Rollup framework. It features a modular design where execution, settlement, and data availability are decoupled. For data availability, it integrates EigenDA, allowing the network to remain efficient and scalable while maintaining Ethereum compatibility.

The following applies to Arbitrum:

The Arbitrum Rollup network operates as a Layer 2 protocol suite built on Ethereum and implemented through the Arbitrum Nitro technology stack. The following description is based on publicly available technical documentation and open source specifications and is provided for informational purposes only; protocol parameters, implementations, and governance processes may change over time.

1. Core protocol architecture (Nitro stack and rollup design)

- Arbitrum Nitro stack: The protocol is implemented through the Arbitrum Nitro architecture, which defines the execution and system components used to process Layer 2 transactions and interface with Ethereum.

- Optimistic rollup model (Arbitrum Rollup): In the rollup configuration (for example, Arbitrum One), transaction data is posted to Ethereum as the parent chain, and the protocol relies on an optimistic execution model with dispute resolution on Ethereum for correctness enforcement.

- Data availability variant (AnyTrust): Arbitrum also defines an AnyTrust configuration (for example, Arbitrum Nova) in which transaction data availability is provided by a Data Availability Committee

(DAC) using signed certificates, with fallback behaviour that can revert to parent chain posting when required by the protocol configuration.

2. Dispute resolution and validation protocol standards

- BoLD dispute protocol: The BoLD (Bounded Liquidity Delay) protocol is specified as a dispute resolution mechanism intended to enable permissionless validation in an optimistic rollup setting.

- On-chain adjudication on the parent chain: Dispute resolution logic is implemented through smart contracts on the parent chain, with participants interacting with those contracts to progress and adjudicate disputes.

- Commitments and proofs: Public documentation describes asserted state commitments and dispute steps that use cryptographic commitments and proof constructions (including Merkle-based commitments and one-step style execution proofs) for resolving contested execution claims on the parent chain.

3. Governance and formal change process (AIP framework)

- Arbitrum Improvement Proposals (AIPs): Formal changes to governance rules, core parameters, and other DAO-controlled actions follow the AIP framework, including an initial forum and Snapshot based temperature check phase and a subsequent on-chain voting phase executed via governance contracts (commonly through Tally's interface).

- Proposal categorisation: AIPs are categorised in documentation (including "Constitutional" and "Non-Constitutional" proposal types) with different scopes of effect as defined by the Arbitrum DAO documentation.

4. Cryptographic primitives and data integrity mechanisms

- Hashing: The protocol and governance documentation uses standard Ethereum-compatible hashing primitives, including keccak256, for certain integrity references (for example, document hashing in governance artefacts).

- BLS signatures for AnyTrust DAC certificates: AnyTrust documentation specifies that DAC membership is represented via keysets and that Data Availability Certificates (DACerts) use BLS public keys and threshold signing assumptions.

- Merkle commitments and proofs: Public specifications describe the use of Merkle commitments and Merkle proofs for state commitment structures and cross-chain messaging verification mechanisms.

- Compression: Nitro documentation describes batch and data handling components that include compression techniques for posting data to the parent chain, with commonly referenced implementations using Brotli compression.

5. Networking interfaces and client interaction standards

- RPC endpoints: Users and integrators interact with Arbitrum chains through JSON-RPC style endpoints compatible with Ethereum tooling patterns.

- Sequencer feed (operational interface): Documentation describes a sequencer broadcast mechanism (including WebSocket-based feeds) that provides near real-time transaction ordering information to clients; this interface is operational and does not constitute a separate consensus protocol of the Layer 2.

The following applies to BNB Chain:

Binance Smart Chain (BSC) is a Layer-1 blockchain that utilises a Proof-of-Staked-Authority (PoSA) consensus mechanism. This mechanism combines elements of Proof-of-Authority (PoA) and Delegated-Proof-of-Stake (DPoS) 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 Base:

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

The following applies to Polygon PoS:

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 Optimism:

Optimism is a Layer 2 scaling solution built on Ethereum that uses Optimistic Rollups technology. Transactions are bundled outside the Ethereum main chain and only transmitted to Layer 1 in compressed form. This significantly reduces gas fees and increases transaction speed. Optimism is fully EVM-compatible and allows developers to migrate existing Ethereum smart contracts without

major adjustments. Optimism's architecture is based on a modular rollup design, with data and execution layers treated separately to ensure scalability and flexibility.

The following applies to Fantom (scheduled for retirement on 30 June 2026):

The legacy Fantom network is EVM-compatible and supports common Ethereum technical standards, including ERC-20 and ERC-721. It uses the Lachesis protocol layer for consensus and supports interoperability with Ethereum tooling and smart contracts. Following the completed migration from Fantom (FTM) to Sonic (S) on 10 May 2025, this description should be read in the context of Fantom as transitional legacy infrastructure rather than the primary forward-looking network.

The following applies to Avalanche C-Chain:

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 in scope is implemented on Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

The following applies to Axelar:

1. Decentralised ledger

The Axelar network operates as a decentralised Proof-of-Stake blockchain built using the Cosmos SDK. The network records transactions and protocol messages in an append-only blockchain structure. Blocks are validated and finalised through CometBFT, a Byzantine Fault Tolerant consensus mechanism, with the intention of maintaining a consistent and transparent record of account balances, staking positions, governance actions, and cross-chain message validation.

2. Cross-chain infrastructure

Axelar is designed to function as a cross-chain communication layer. Its infrastructure includes the Axelar blockchain, validators, relayers, gateway contracts or gateway applications on connected external networks, and services that assist with cross-chain gas payment and execution. In practical terms, the Axelar blockchain acts as the coordination layer, while gateways and relayers connect this coordination layer to external blockchain environments.

Cross-chain messages are tracked using transaction hashes, payload hashes, and chain-specific event data. Validators verify relevant events from connected chains before the network authorises execution on a destination chain. This allows Axelar to support cross-chain transfers and general message passing between otherwise independent networks.

3. Smart-contract and execution environment

The Axelar network supports programmable cross-chain logic through the Axelar Virtual Machine, which is powered by CosmWasm. CosmWasm enables smart contracts to be deployed on the Axelar network for the purpose of implementing application-level rules and cross-chain workflows. Developers may also interact with Axelar from external Ethereum-compatible networks through Solidity-based gateway contracts and from other environments through supported software development kits.

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. In addition, BLS (Boneh-Lynn-Shacham) signatures are used for validator aggregation in PoS.

The following applies to Osmosis:

The platform functions as an automated market maker (AMM) with customisable liquidity pools. Osmosis leverages the Tendermint Core consensus engine and Cosmos SDK modules, which provide modularity and extensibility. While this design supports innovation, it also increases the attack surface, and the AMM model itself remains sensitive to issues such as front-running, slippage, and smart contract vulnerabilities.

The following applies to Linea:

The Linea protocol is a Type 2 Zero-Knowledge Ethereum Virtual Machine (zkEVM) network that aims to scale Ethereum while preserving its security and developer experience. The network is designed for full EVM equivalence at the bytecode level, which is a critical standard for seamless interoperability. As a zk-rollup, the network utilises zero-knowledge proofs (ZKPs) to ensure the integrity of off-chain transactions. The network uses a custom, in-house proving system based on recursive SNARKs, with components named Arcane and Vortex. This system is used to generate validity proofs that confirm off-chain computations are correct. The network uses lattice-based cryptography for its ZKPs, which offers resistance to potential threats from quantum computing.

The network's off-chain execution environment uses data structures that mirror Ethereum's own state management. The network uses a Merkle-Patricia Trie to record the world state and manage consensus, just as Ethereum does. To improve efficiency in tracking and updating account storage, LINEA protocol uses a sparse Merkle tree.

The following applies to Mantle:

Mantle implements a modular blockchain architecture that separates execution (via the EVM), data availability (via EigenDA), and settlement (on Ethereum). This approach enhances scalability, reduces transaction costs, and ensures compatibility with existing Ethereum tooling. It also uses multi-party computation to reduce withdrawal times of the optimistic rollup.

The following applies to Arbitrum:

1. Arbitrum-compatible wallets: Tokens on Arbitrum are usable with standard Ethereum-compatible wallets that support EVM chains (for example, MetaMask) via the network's RPC endpoints.

2. Decentralised ledger and L1 settlement: Arbitrum maintains an account-based ledger and state as a Layer 2 chain, with transaction data posted to Ethereum Layer 1 in batches in rollup mode (including via calldata and, where configured, EIP-4844 blob transactions).

3. ERC-20 token standard: Arbitrum is EVM-compatible through the Nitro stack (built around a modified Geth core), and therefore supports standard EVM token interfaces such as ERC-20.

4. Multi-VM execution environment: In addition to EVM execution, Arbitrum supports a co-located WASM virtual machine via Stylus, enabling smart contract execution for WASM-compiled languages alongside EVM contracts.

5. Scalability and transaction efficiency design: As an optimistic rollup architecture, Arbitrum is designed to execute transactions on Layer 2 and publish the relevant data to Ethereum, with correctness enforcement and protocol security mechanisms anchored to the parent chain.

The following applies to BNB 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. Decentralised 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 Base:

1. Base-compatible wallets: The tokens are supported by all wallets compatible with the Ethereum Virtual Machine (EVM), such as MetaMask, Coinbase Wallet, and Trust Wallet. These wallets interact with Base in the same way as with other EVM-compatible chains, using standard Web3 interfaces.

2. Decentralised ledger: Base operates as a Layer-2 blockchain on Ethereum and maintains its own decentralised ledger for recording token transactions. Final transaction data is periodically posted to Ethereum Layer 1, ensuring long-term availability and resistance to tampering.

3. ERC-20 token standard: The Base network supports tokens implemented under the ERC-20 standard, the same as on Ethereum.

4. Scalability and transaction efficiency:

As a rollup-based Layer-2, Base is intended to handle high volumes of transactions with lower fees compared to Ethereum Layer 1. This is enabled by off-chain execution and on-chain data posting via an optimistic rollup architecture.

The following applies to Polygon PoS:

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 Optimism:

Optimism is fully compatible with Ethereum tooling and supports common smart-contract languages and frameworks, including Solidity, Vyper, Hardhat, Foundry, and Truffle. This allows developers to deploy their applications on Optimism without making major changes. In addition, the bridge between Ethereum and Optimism is designed to allow assets to be easily transferred between the two networks.

The following applies to Fantom (scheduled for retirement on 30 June 2026):

The legacy Fantom Opera network uses a Directed Acyclic Graph (DAG)-based architecture powered by the Lachesis protocol to support fast transaction confirmation and network scalability. Following the completed migration from Fantom (FTM) to Sonic (S) on 10 May 2025, this description should be read in the context of Fantom Opera as transitional legacy infrastructure rather than the primary forward-looking network.

The following applies to Avalanche C-Chain:

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 in scope is implemented on Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

The following applies to Axelar:

The Axelar network operates a Proof-of-Stake consensus mechanism based on CometBFT, formerly Tendermint consensus. CometBFT is a Byzantine Fault Tolerant consensus algorithm designed to provide deterministic block finality and consistent state replication among validators.

Consensus participants are validators who bond the native crypto-asset AXL and obtain voting power based on their bonded stake, including AXL delegated to them by third parties. Validators participate in block production and consensus by proposing blocks, verifying transactions, and broadcasting cryptographic votes. Token holders may delegate AXL to validators, thereby contributing to the validator's voting power without operating validator infrastructure themselves.

Consensus proceeds in rounds, each consisting of a block proposal followed by two voting phases, commonly referred to as pre-vote and pre-commit. A block is finalised and committed once more than two-thirds of the total validator voting power pre-commits to the same block in the same round. This mechanism provides deterministic finality for the Axelar blockchain and does not rely on probabilistic fork resolution.

In addition to base-layer block consensus, Axelar uses threshold signature schemes for cross-chain authorisation. Validators participate in multi-party cryptographic processes that allow the network to authorise commands on connected external chains. Under this model, gateway signing authority is divided into key shares held by validators, and cross-chain execution requires participation by the required threshold of validator voting power.

Axelar validators may also verify events from connected external blockchains. For this purpose, validators may run or access nodes for supported external chains and use those sources to confirm that relevant events have occurred before voting on their validity within the Axelar network. Cross-chain messages therefore depend both on Axelar's own consensus finality and on the finality properties of the source chain from which a message originates.

CometBFT provides Byzantine Fault Tolerance, meaning that the network is designed to remain safe and consistent as long as less than one-third of total validator voting power behaves maliciously or fails. For cross-chain actions, Axelar additionally relies on threshold cryptography and validator participation requirements to reduce the risk that a single validator or operator can unilaterally authorise transactions on connected chains.

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 Osmosis:

Osmosis applies a Proof-of-Stake consensus through the Tendermint BFT engine. Validator nodes secure the network by staking OSMO tokens, and consensus is reached with fast finality. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behaviour. The system may be exposed to validator collusion or governance capture.

The following applies to Linea:

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

The following applies to Mantle:

The Mantle Network does not operate a native Layer 1 consensus mechanism. As an Ethereum Layer 2 network, it relies on Ethereum for settlement and dispute resolution, while using a modular architecture in which execution, settlement, and data availability are separated. Transaction data or data-availability commitments are handled through Mantle's data-availability architecture, including EigenDA, while correctness of Layer 2 execution is addressed through the applicable rollup and dispute-resolution mechanisms.

The following applies to Arbitrum:

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

The following applies to BNB 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 is intended to support fast block times and low fees while maintaining a level of decentralisation and security.

Core components

1. Validators (Cabinet and Candidates): Validators are responsible for producing blocks, validating transactions, and maintaining network security. The validator set consists of up to 45 validators, including 21 “Cabinet” validators and 24 “Candidate” validators, selected based on bonded stake. A subset of validators is selected per epoch to participate in block production.

2. Delegators: Token holders may delegate BNB to validators to support their selection. Delegators share in the rewards generated by validators, providing an economic incentive to participate in staking.

3. Candidates: Validator candidates are nodes that have staked BNB but are not part of the primary validator subset for a given epoch. They may be selected into the active set based on staking rank and can participate in block production with lower probability.

Consensus process

4. Validator selection: Validators are ranked based on the amount of bonded BNB and are updated periodically (approximately every 24 hours). The highest-ranked validators form the active validator set, with Cabinet validators having a higher probability of participating in block production.

5. Block production: Validators take turns producing blocks in a PoA-like manner. For each epoch, a subset of validators is selected to produce and validate blocks sequentially, ensuring high throughput and low latency.

6. Transaction finality: BSC achieves short block times (approximately 0.45 seconds) and fast finality. With Fast Finality enabled, blocks are typically finalised within approximately one second, subject to validator participation.

7. Staking: Validators must stake BNB as collateral and may be subject to slashing in cases of misbehaviour, including double-signing, malicious voting, or prolonged downtime.

8. Delegation and rewards: Validators and delegators are rewarded through transaction fees collected in each block. Validators may share rewards with delegators to attract stake.

9. Transaction fees: BSC does not rely on inflationary block rewards; instead, validators are compensated primarily through transaction fees paid in BNB, aligning incentives with network usage.

The following applies to Base:

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

The following applies to Polygon PoS:

Polygon PoS is an EVM-compatible sidechain that operates with a Proof-of-Stake (PoS) consensus mechanism and periodically submits checkpoints to the Ethereum mainnet. The network maintains its own validator set and processes transactions independently from Ethereum, while using Ethereum as a settlement and checkpointing layer. The architecture consists of two primary layers:

- Bor layer (execution layer): Responsible for block production and transaction execution. A subset of validators is selected to act as block producers for defined periods, during which they create and propagate blocks across the network.

- Heimdall layer (consensus layer): Responsible for validator coordination, staking management, and checkpoint finalisation. Heimdall is based on CometBFT and aggregates blocks produced by Bor into periodic checkpoints.

Validators participate in the network by staking POL tokens. The probability of being selected as a block producer is influenced by the validator's stake. Token holders may delegate their tokens to validators, contributing to their effective stake and participating indirectly in network validation. Delegators may receive a share of rewards generated by validators.

Transactions are executed on the Bor layer and validated by the active set of block producers. At regular intervals, Heimdall validators aggregate blocks into a Merkle root and submit this checkpoint to smart contracts on the Ethereum mainnet. These checkpoints provide an additional layer of security and enable cross-chain verification, particularly in the context of asset transfers between Polygon PoS and Ethereum.

This design allows Polygon PoS to achieve high throughput and reduced transaction costs while maintaining a connection to Ethereum through periodic checkpointing. However, the network does not rely on Ethereum for full transaction data availability or execution, and therefore operates as an independent sidechain rather than a Layer 2 rollup.

The following applies to Optimism:

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

The following applies to Fantom (scheduled for retirement on 30 June 2026):

The legacy Fantom network uses the Lachesis consensus protocol, an asynchronous Byzantine Fault Tolerant consensus mechanism. Following the completed migration from Fantom (FTM) to Sonic (S) on 10 May 2025, the main network focus has shifted to Sonic. Accordingly, this description should be read in the context of Fantom as legacy infrastructure rather than the primary forward-looking network.

The following applies to Avalanche C-Chain:

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 $\alpha = 14$, and decision threshold $\beta = 20$, 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 in scope is implemented on Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

The following applies to Axelar:

The Axelar network secures its Proof-of-Stake consensus mechanism through staking rewards, transaction fees, and penalties. Validators and delegators are incentivised to participate honestly in block production, transaction validation, and cross-chain message verification.

Validators and delegators may receive rewards in AXL. These rewards are generally derived from inflationary issuance and applicable network fees and are distributed in proportion to bonded stake, subject to validator commission rates and network parameters. Validators may also receive additional incentives for supporting external blockchain connections, including by operating or accessing infrastructure required to verify cross-chain events.

Users pay transaction fees for activity on the Axelar network. Cross-chain transactions may also require fees for source-chain execution, Axelar network processing, relayer activity, and destination-chain execution. These fees may be handled through the Axelar Gas Service, which is used to support payment and execution across connected chains.

Collected fees may be distributed to validators and delegators, allocated to network-controlled pools, or burned, depending on the applicable protocol rules and governance-approved parameters. Bonded AXL may be subject to slashing or other penalties where validators fail to comply with protocol rules, including downtime, double-signing, or other conduct that affects consensus or cross-chain security.

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 Osmosis:

The network incentivises liquidity providers and validators through block rewards and transaction fees paid in OSMO. Liquidity mining programs and governance-driven reward distribution may influence participation but can also result in centralisation of liquidity or speculative behaviour. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

The following applies to Linea:

Like Ethereum, the network uses a gas system, where gas is the unit of computational effort required to process a transaction. All gas fees on the network are paid in Ether (ETH). The network has a base fee that is designed to stabilise at 7 wei. The base fee still decreases or increases based on network traffic, similar to Ethereum, but it does not go below 7 wei.

The network does not require token staking for transaction validation purposes and thus provides no staking rewards. It does not offer incentives for running a full network node. It does charge fees collected by the sequencer for transaction processing. Those fees are paid in ETH, 20% of which are immediately burned while the remaining 80% are converted to Tokens and then burned.

The following applies to Mantle:

Participants in the Mantle ecosystem, such as sequencers and data availability providers, are incentivised through network fees. Thanks to the modular setup and off-chain execution, transaction fees are significantly reduced compared to Ethereum mainnet. To get crypto-assets in and out of Mantle, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2, an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains undisputed for a period of time the funds can be withdrawn. During this time period Mantle validators can dispute the claim, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour of all participants.

The following applies to Arbitrum:

Arbitrum is a Layer-2 (L2) solution on Ethereum that is developed using the Arbitrum technology suite. Transactions on Arbitrum are bundled by a so-called sequencer and the result is regularly submitted as a Layer-1 (L1) transaction. This way many L2 transactions are combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use Arbitrum rather than the L1, i.e. Ethereum, itself. To get crypto-assets in and out of Arbitrum, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2, an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains undisputed for a period of time the funds can be withdrawn. During this time period Arbitrum validators can dispute the claim, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour of all participants.

The following applies to BNB Chain:

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

Incentive mechanisms

1. Validators: Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure.

2. Delegators: BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission.

3. Candidates: BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information.

4. Economic Security: Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance.

Fees on the Binance Smart Chain

5. Transaction fees: Transaction fees on BSC are paid in BNB and are intended to compensate validators for maintaining the network. BSC is designed as a comparatively low-fee network, and smart-contract transactions and transfers require gas fees in BNB.

6. Validator rewards: BSC does not rely on a separate protocol-level block reward. Instead, staking rewards are derived from transaction fees. Most of the block fee is allocated to the proposing validator, then split between validator commission and delegator-linked reward distribution.

7. System-level fee allocation: Part of transaction-fee revenue is collected through the System Reward Contract and used for designated system purposes, including fast-finality rewards.

8. Smart contract fees: Deploying and interacting with smart contracts on BSC requires payment of gas fees in BNB. These fees depend on the computational resources required and form part of the network's overall fee and validator-incentive model.

The following applies to Base:

Base is a Layer-2 (L2) solution on Ethereum that uses optimistic rollups provided by the OP Stack on which it was developed. Transactions on Base are bundled by a so-called sequencer, and the result is regularly submitted as Layer-1 (L1) transactions. This way, many L2 transactions are combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use Base rather than the L1, i.e. Ethereum, itself. To move crypto-assets in and out of Base, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2, an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, the user needs to submit a withdrawal request on L1. If this request remains unchallenged for a period of time, the funds can be withdrawn. During this period, any other user can submit a fault proof, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour.

The following applies to Polygon PoS:

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 increases. 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 Optimism:

Optimism charges significantly lower transaction fees than Ethereum Layer 1, as transactions are bundled in the rollup and written to the Ethereum main chain in compressed form. Gas fees on Optimism continue to be paid in ETH.

The incentive model is based on increased efficiency for users (lower fees, faster confirmation) and on the role of sequencers. Sequencers are central actors who collect, organise, and include transactions in the rollup. Their revenue comes from the gas fees they charge. Fault proofs ensure that sequencers cannot permanently enforce incorrect or malicious transactions. Fault proofs and their resolution are also incentivised economically to discourage faults to begin with.

The following applies to Fantom (scheduled for retirement on 30 June 2026):

The legacy Fantom network has used staking-based incentive mechanisms under which validators and delegators may receive FTM rewards for participating in network security. Following the completed migration from Fantom (FTM) to Sonic (S) on 10 May 2025, these mechanisms should be read in the context of Fantom as transitional legacy infrastructure rather than the primary forward-looking network.

The following applies to Avalanche C-Chain:

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 – 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.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

Given the breadth of the term "technology", it cannot be confirmed that all elements or aspects of the technology employed have undergone a comprehensive and systematic technical examination. Accordingly, no comprehensive audit of the technology used can be confirmed. 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 venues on which it is listed 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 where 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 listing crypto-asset 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 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 transaction 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

1. Insolvency of the issuer

As with any commercial entity, the issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, or external shocks (e.g. pandemics, armed conflicts). In such a case, ongoing development, support, and governance of the project may cease, potentially affecting the viability and 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 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. Crypto-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, reporting 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 admission to trading of the crypto-asset, the risk description below reflects general implementation risks typically associated with crypto-asset projects and relevant for the crypto-asset service provider. The party admitting the crypto-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 crypto-asset's practical utility.

I.5 Technology-related risks

As this white paper relates to 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 the 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

Axelar

S.4 Consensus Mechanism

The crypto-asset in scope is implemented on Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

The following applies to Axelar:

The Axelar network operates a Proof-of-Stake consensus mechanism based on CometBFT, formerly Tendermint consensus. CometBFT is a Byzantine Fault Tolerant consensus algorithm designed to provide deterministic block finality and consistent state replication among validators.

Consensus participants are validators who bond the native crypto-asset AXL and obtain voting power based on their bonded stake, including AXL delegated to them by third parties. Validators participate in block production and consensus by proposing blocks, verifying transactions, and broadcasting cryptographic votes. Token holders may delegate AXL to validators, thereby contributing to the validator's voting power without operating validator infrastructure themselves.

Consensus proceeds in rounds, each consisting of a block proposal followed by two voting phases, commonly referred to as pre-vote and pre-commit. A block is finalised and committed once more than two-thirds of the total validator voting power pre-commits to the same block in the same round. This mechanism provides deterministic finality for the Axelar blockchain and does not rely on probabilistic fork resolution.

In addition to base-layer block consensus, Axelar uses threshold signature schemes for cross-chain authorisation. Validators participate in multi-party cryptographic processes that allow the network to authorise commands on connected external chains. Under this model, gateway signing authority is divided into key shares held by validators, and cross-chain execution requires participation by the required threshold of validator voting power.

Axelar validators may also verify events from connected external blockchains. For this purpose, validators may run or access nodes for supported external chains and use those sources to confirm that relevant events have occurred before voting on their validity within the Axelar network. Cross-

chain messages therefore depend both on Axelar's own consensus finality and on the finality properties of the source chain from which a message originates.

CometBFT provides Byzantine Fault Tolerance, meaning that the network is designed to remain safe and consistent as long as less than one-third of total validator voting power behaves maliciously or fails. For cross-chain actions, Axelar additionally relies on threshold cryptography and validator participation requirements to reduce the risk that a single validator or operator can unilaterally authorise transactions on connected chains.

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 Osmosis:

Osmosis applies a Proof-of-Stake consensus through the Tendermint BFT engine. Validator nodes secure the network by staking OSMO tokens, and consensus is reached with fast finality. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behaviour. The system may be exposed to validator collusion or governance capture.

The following applies to Linea:

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

The following applies to Mantle:

The Mantle Network does not operate a native Layer 1 consensus mechanism. As an Ethereum Layer 2 network, it relies on Ethereum for settlement and dispute resolution, while using a modular architecture in which execution, settlement, and data availability are separated. Transaction data or data-availability commitments are handled through Mantle's data-availability architecture, including

EigenDA, while correctness of Layer 2 execution is addressed through the applicable rollup and dispute-resolution mechanisms.

The following applies to Arbitrum:

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

The following applies to BNB 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 is intended to support fast block times and low fees while maintaining a level of decentralisation and security.

Core components

1. Validators (Cabinet and Candidates): Validators are responsible for producing blocks, validating transactions, and maintaining network security. The validator set consists of up to 45 validators, including 21 “Cabinet” validators and 24 “Candidate” validators, selected based on bonded stake. A subset of validators is selected per epoch to participate in block production.

2. Delegators: Token holders may delegate BNB to validators to support their selection. Delegators share in the rewards generated by validators, providing an economic incentive to participate in staking.

3. Candidates: Validator candidates are nodes that have staked BNB but are not part of the primary validator subset for a given epoch. They may be selected into the active set based on staking rank and can participate in block production with lower probability.

Consensus process

4. Validator selection: Validators are ranked based on the amount of bonded BNB and are updated periodically (approximately every 24 hours). The highest-ranked validators form the active validator set, with Cabinet validators having a higher probability of participating in block production.

5. Block production: Validators take turns producing blocks in a PoA-like manner. For each epoch, a subset of validators is selected to produce and validate blocks sequentially, ensuring high throughput and low latency.

6. Transaction finality: BSC achieves short block times (approximately 0.45 seconds) and fast finality. With Fast Finality enabled, blocks are typically finalised within approximately one second, subject to validator participation.

7. Staking: Validators must stake BNB as collateral and may be subject to slashing in cases of misbehaviour, including double-signing, malicious voting, or prolonged downtime.

8. Delegation and rewards: Validators and delegators are rewarded through transaction fees collected in each block. Validators may share rewards with delegators to attract stake.

9. Transaction fees: BSC does not rely on inflationary block rewards; instead, validators are compensated primarily through transaction fees paid in BNB, aligning incentives with network usage.

The following applies to Base:

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

The following applies to Polygon PoS:

Polygon PoS is an EVM-compatible sidechain that operates with a Proof-of-Stake (PoS) consensus mechanism and periodically submits checkpoints to the Ethereum mainnet. The network maintains its own validator set and processes transactions independently from Ethereum, while using Ethereum as a settlement and checkpointing layer. The architecture consists of two primary layers:

- Bor layer (execution layer): Responsible for block production and transaction execution. A subset of validators is selected to act as block producers for defined periods, during which they create and propagate blocks across the network.

- Heimdall layer (consensus layer): Responsible for validator coordination, staking management, and checkpoint finalisation. Heimdall is based on CometBFT and aggregates blocks produced by Bor into periodic checkpoints.

Validators participate in the network by staking POL tokens. The probability of being selected as a block producer is influenced by the validator's stake. Token holders may delegate their tokens to validators, contributing to their effective stake and participating indirectly in network validation. Delegators may receive a share of rewards generated by validators.

Transactions are executed on the Bor layer and validated by the active set of block producers. At regular intervals, Heimdall validators aggregate blocks into a Merkle root and submit this checkpoint to smart contracts on the Ethereum mainnet. These checkpoints provide an additional layer of

security and enable cross-chain verification, particularly in the context of asset transfers between Polygon PoS and Ethereum.

This design allows Polygon PoS to achieve high throughput and reduced transaction costs while maintaining a connection to Ethereum through periodic checkpointing. However, the network does not rely on Ethereum for full transaction data availability or execution, and therefore operates as an independent sidechain rather than a Layer 2 rollup.

The following applies to Optimism:

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

The following applies to Fantom (scheduled for retirement on 30 June 2026):

The legacy Fantom network uses the Lachesis consensus protocol, an asynchronous Byzantine Fault Tolerant consensus mechanism. Following the completed migration from Fantom (FTM) to Sonic (S) on 10 May 2025, the main network focus has shifted to Sonic. Accordingly, this description should be read in the context of Fantom as legacy infrastructure rather than the primary forward-looking network.

The following applies to Avalanche C-Chain:

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 $\alpha = 14$, and decision threshold $\beta = 20$, 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 in scope is implemented on Axelar (native), Ethereum, Osmosis, Linea, Mantle, Arbitrum, BNB Chain, Base, Polygon PoS, Optimism, Fantom and Avalanche C-Chain networks following the standards described below.

The following applies to Axelar:

The Axelar network secures its Proof-of-Stake consensus mechanism through staking rewards, transaction fees, and penalties. Validators and delegators are incentivised to participate honestly in block production, transaction validation, and cross-chain message verification.

Validators and delegators may receive rewards in AXL. These rewards are generally derived from inflationary issuance and applicable network fees and are distributed in proportion to bonded stake, subject to validator commission rates and network parameters. Validators may also receive additional incentives for supporting external blockchain connections, including by operating or accessing infrastructure required to verify cross-chain events.

Users pay transaction fees for activity on the Axelar network. Cross-chain transactions may also require fees for source-chain execution, Axelar network processing, relayer activity, and destination-chain execution. These fees may be handled through the Axelar Gas Service, which is used to support payment and execution across connected chains.

Collected fees may be distributed to validators and delegators, allocated to network-controlled pools, or burned, depending on the applicable protocol rules and governance-approved parameters. Bonded AXL may be subject to slashing or other penalties where validators fail to comply with protocol rules, including downtime, double-signing, or other conduct that affects consensus or cross-chain security.

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 Osmosis:

The network incentivises liquidity providers and validators through block rewards and transaction fees paid in OSMO. Liquidity mining programs and governance-driven reward distribution may influence participation but can also result in centralisation of liquidity or speculative behaviour. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

The following applies to Linea:

Like Ethereum, the network uses a gas system, where gas is the unit of computational effort required to process a transaction. All gas fees on the network are paid in Ether (ETH). The network has a base fee that is designed to stabilise at 7 wei. The base fee still decreases or increases based on network traffic, similar to Ethereum, but it does not go below 7 wei.

The network does not require token staking for transaction validation purposes and thus provides no staking rewards. It does not offer incentives for running a full network node. It does charge fees collected by the sequencer for transaction processing. Those fees are paid in ETH, 20% of which are immediately burned while the remaining 80% are converted to Tokens and then burned.

The following applies to Mantle:

Participants in the Mantle ecosystem, such as sequencers and data availability providers, are incentivised through network fees. Thanks to the modular setup and off-chain execution, transaction fees are significantly reduced compared to Ethereum mainnet. To get crypto-assets in and out of Mantle, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2, an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains undisputed for a period of time the funds can be withdrawn. During this time period Mantle validators can dispute the claim, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour of all participants.

The following applies to Arbitrum:

Arbitrum is a Layer-2 (L2) solution on Ethereum that is developed using the Arbitrum technology suite. Transactions on Arbitrum are bundled by a so-called sequencer and the result is regularly submitted as a Layer-1 (L1) transaction. This way many L2 transactions are combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use Arbitrum rather than the L1, i.e. Ethereum, itself. To get crypto-assets in and out of Arbitrum, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2, an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains undisputed for a period of time the funds can be withdrawn. During this time period Arbitrum validators can dispute the claim, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour of all participants.

The following applies to BNB Chain:

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

Incentive mechanisms

1. Validators: Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure.

2. Delegators: BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission.

3. Candidates: BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information.

4. Economic Security: Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance.

Fees on the Binance Smart Chain

5. Transaction fees: Transaction fees on BSC are paid in BNB and are intended to compensate validators for maintaining the network. BSC is designed as a comparatively low-fee network, and smart-contract transactions and transfers require gas fees in BNB.

6. Validator rewards: BSC does not rely on a separate protocol-level block reward. Instead, staking rewards are derived from transaction fees. Most of the block fee is allocated to the proposing validator, then split between validator commission and delegator-linked reward distribution.

7. System-level fee allocation: Part of transaction-fee revenue is collected through the System Reward Contract and used for designated system purposes, including fast-finality rewards.

8. Smart contract fees: Deploying and interacting with smart contracts on BSC requires payment of gas fees in BNB. These fees depend on the computational resources required and form part of the network's overall fee and validator-incentive model.

The following applies to Base:

Base is a Layer-2 (L2) solution on Ethereum that uses optimistic rollups provided by the OP Stack on which it was developed. Transactions on Base are bundled by a so-called sequencer, and the result is regularly submitted as Layer-1 (L1) transactions. This way, many L2 transactions are combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use Base rather than the L1, i.e. Ethereum, itself. To move crypto-assets in and out of Base, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2, an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, the user needs to submit a withdrawal request on L1. If this request remains unchallenged for a period of time, the funds can be withdrawn. During this period, any other user can submit a fault proof, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour.

The following applies to Polygon PoS:

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 increases. 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 Optimism:

Optimism charges significantly lower transaction fees than Ethereum Layer 1, as transactions are bundled in the rollup and written to the Ethereum main chain in compressed form. Gas fees on Optimism continue to be paid in ETH.

The incentive model is based on increased efficiency for users (lower fees, faster confirmation) and on the role of sequencers. Sequencers are central actors who collect, organise, and include transactions in the rollup. Their revenue comes from the gas fees they charge. Fault proofs ensure that sequencers cannot permanently enforce incorrect or malicious transactions. Fault proofs and their resolution are also incentivised economically to discourage faults to begin with.

The following applies to Fantom (scheduled for retirement on 30 June 2026):

The legacy Fantom network has used staking-based incentive mechanisms under which validators and delegators may receive FTM rewards for participating in network security. Following the completed migration from Fantom (FTM) to Sonic (S) on 10 May 2025, these mechanisms should be read in the context of Fantom as transitional legacy infrastructure rather than the primary forward-looking network.

The following applies to Avalanche C-Chain:

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

2025-04-30

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

2026-04-30

S.8 Energy consumption

29932.56711 kWh/a

S.9 Energy consumption sources and methodologies

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

For the calculation of energy consumption, the so-called 'bottom-up' approach is being used. The nodes are considered to be the central factor for the energy consumption of the network. These assumptions are made on the basis of empirical findings through the use of public information sites, open-source crawlers and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the client software. The energy consumption of the hardware devices was measured in certified test laboratories. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset in scope and we update the mappings regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

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

S.10 Renewable energy consumption

34.9073642851 %

S.11 Energy intensity

0.00007 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

9.96195 tCO2e/a

S.14 GHG intensity

0.00002 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.