CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG 2HZXZQLKX

Preamble

00. Table of Content

01. Date of notification

This white paper was notified at 2026-03-06.

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 KAVA referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed on the Kava network and also represented on the Ethereum, Binance Beacon Chain (shut down), Polygon, and Osmosis networks, according to the DTI FFG shown in section F.14, as of 2026-03-02.

The maximum supply of the crypto-asset is 1,080,000,000 tokens. The first activity on Kava can be viewed on 2022-05-25 (block hash: 0x9d2af876309bb9174604004a813dcfee94f4947b08c5bb4c1a042f318488851e, source: https://kavascan.io/block/1, accessed 2026-03-02). The first activity on Ethereum can be viewed on 2021-09-03 (transaction hash: 0xbc2c73fe0616eac0e224fa653b368436b65dc2666718956cb22644696ce7ced8, source: https://etherscan.io/tx/0xbc2c73fe0616eac0e224fa653b368436b65dc2666718956cb22644696ce7ced8, accessed 2026-03-02). The Binance Beacon Chain was shut down in December 2024, therefore no activity of Kava can be retrieved. The first activity on Polygon can be viewed on 2021-09-11 (transaction hash: 0x121c10f433b235841b519b6fd8a6ac7301694d48e972c8c812ccf4088cad4ffe, source: https://polygonscan.com/tx/0x121c10f433b235841b519b6fd8a6ac7301694d48e972c8c812ccf4088cad4ffe, accessed 2026-03-02). The first activity on Osmosis can be viewed on 2022-01-20 (relayer: OSMOSIS / channel-143, source: https://www.mintscan.io/osmosis/relayers/channel-143/kava/channel-1?sector=status, accessed 2026-03-02).

Kava is a decentralised, permissionless Layer-1 blockchain project designed to support smart-contract applications and token transfers across multiple ecosystems by combining an Ethereum-compatible execution environment with the Cosmos SDK interoperability stack. The Kava Network is implemented using a co-chain architecture, consisting of an Ethereum Virtual Machine (EVM) co-chain for Solidity-based decentralised application deployment and a Cosmos co-chain leveraging Tendermint Core consensus and Inter-Blockchain Communication (IBC) to connect with other IBC-enabled networks. The two execution environments interoperate through protocol modules that facilitate asset and data movement between the EVM and Cosmos components of the network. The protocol further supports an internal bridging mechanism that enables the representation of Cosmos-native tokens in ERC-20 format for use in the EVM environment. Network governance and parameter management are performed through a DAO-style on-chain governance process involving validators and token holders.

The KAVA crypto-asset functions as the native governance, staking, and utility token of the Kava Network and is used within protocol-defined mechanisms related to network security, transaction processing, and on-chain governance. Under the network's Proof-of-Stake model, validator nodes bond KAVA and may be subject to slashing conditions for specified validator misbehaviour, while validators and delegators may receive rewards funded through transaction fees and protocol-defined distributions. KAVA may be used to participate in governance processes, including proposing and voting on changes to protocol parameters and risk settings for protocol modules, where applicable. KAVA also serves as a gas and fee token for transactions conducted on the network's execution environments, and can be wrapped into an EVM-compatible representation (WKAVA) for use in EVM smart contracts. In certain protocol-defined stress scenarios, additional KAVA issuance mechanisms may be used as a backstop to cover system shortfalls, and the protocol transitioned to a zero-inflation model as of 2023-12-31, under which no routine inflation-based issuance is intended and tokens may be removed from supply through burning mechanisms.

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, amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. The admission to trading is not accompanied by a public offer of the crypto-asset.

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

federal state Hamburg.

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

Based on the current business development in Q4 2025, revenues exceeding EUR 550,000 are expected for the fiscal year 2025, with an anticipated net profit of approximately EUR 100,000. These figures are neither audited nor based on a finalised annual financial statement; they are derived from the company's current pipeline, client development, and active commercial engagements. Accordingly, they are subject to future risks and market fluctuations.

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

KAVA LABS INC.

B.3 Legal form

The legal form of KAVA LABS INC. is XTIQ, which corresponds to “Corporation”.

B.4 Registered address

The registered address of KAVA LABS INC. is 8 The Green, Ste A, Dover, DE 19901,

United States,

US-DE

B.5 Head office

The Head Office address of KAVA LABS INC. is 345 California St, Ste 600, San Francisco, CA 94104,

United States,

US-CA

B.6 Registration date

KAVA LABS INC. was registered on 2018-01-10.

B.7 Legal entity identifier

KAVA LABS INC. has no Legal Entity Identifier (LEI).

B.8 Another identifier required pursuant to applicable national law

Delaware File Number: 6703728

B.9 Parent company

No parent company of KAVA LABS INC. can be identified.

B.10 Members of the management body

Identity	Function	Business Address
Brian Kerr	Co-founder and board member of KAVA LABS INC.	345 California St, Ste 600, San Francisco, CA 94104, United States

B.11 Business activity

Kava Labs Inc. develops and operates Web3 financial infrastructure, including a blockchain network and related services that enable users to issue and use virtual currencies, transfer crypto-assets

electronically, exchange cryptocurrencies, and access crypto-based lending products such as stablecoins collateralized by cryptocurrency.

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: "KAVA", Short Name: "KAVA" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-03-03).

D.2 Crypto-assets name

Long Name: "KAVA" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-03-03).

D.3 Abbreviation

Short Name: "KAVA" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-03-03).

D.4 Crypto-asset project description

According to public information published in the Kava documentation (source: https://docs.kava.io/, accessed 2026-03-02), the Kava project is a decentralised Layer-1 blockchain network built to support smart-contract applications and token transfers across multiple ecosystems. The network combines an Ethereum-compatible execution environment with a Cosmos SDK based interoperability stack, enabling developers to deploy EVM smart contracts while also supporting cross-chain transfers via IBC. The protocol operates under a proof-of-stake security model with validator participation and on-chain governance processes used to manage protocol parameters and network operations.

The project does not involve the granting of ownership, profit-participation rights, or legal claims against the project entity or its contributors. Instead, it centres on the creation of a technical environment in which the KAVA crypto-asset may serve as a governance and utility input for certain protocol processes. The long-term evolution of the Kava system, including the scope of available features, the decentralisation roadmap, validator-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
Scott Stuart	Other person involved in implementation	Cannot be found	Cannot be found
Brian Kerr	Other person involved in implementation	Cannot be found	Cannot be found
Ruaridh O'Donnell	Other person involved in implementation	522 W Riverside Ave Ste N, Spokane, WA, 99201-0581, United States	United States
Kava Labs Inc.	Other person involved in implementation	345 California St, Ste 600, San Francisco, CA 94104, US	United States

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

There is a formally published roadmap for the KAVA crypto-asset and the KAVA protocol. Based on the official roadmap (sources: https://www.kava.io/roadmap; accessed 2026-03-02), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Kava protocol and the role of the KAVA crypto-asset.

Past milestones:

- Initial Exchange Offering on Binance Launchpad (October 2019): The project reportedly conducted an IEO on Binance Launchpad, raising approximately USD 3 million.

- IBC integration (19 January 2022): Integration with the Inter-Blockchain Communication protocol was completed.

- Kava 10 Mainnet and Kava EVM launch (25 May 2022): Kava 10 Mainnet launched, including the debut of the Kava EVM, and the project initiated the "Kava Rise" developer incentive program.

- Kava 15 Mainnet and zero inflation milestone (7-31 December 2023): Kava 15 mainnet launched, culminating in a milestone where KAVA inflation was reduced to zero on 31 December 2023.

- USDT liquidity scaling (Q1 2026): The project described plans to accelerate native USDT liquidity through partners to position Kava as a hub for stablecoin settlement.

Future milestones:

- Real World Assets ecosystem launch (Q2 2026): The project described plans to launch a Real World Assets ecosystem and introduce tokenised financial products with transparent accounting.

- Non-USD stablecoin expansion and autonomous agent execution (Q3 2026): The project described plans to expand to non-USD stablecoins (examples referenced include EUR and JPY) and to evolve AI agents toward autonomous execution use cases.

- Fiat onramps and partner distribution expansion (Q4 2026): The project described plans to expand distribution through fiat onramps and partner integrations to enable access to RWA products via credit card purchases.

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 KAVA 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 KAVA token has conducted multiple funding rounds involving private investors and venture capital firms.

According to publicly referenced information, on or around 28 February 2019, the project is reported to have completed a venture capital funding round with an indicated amount of approximately USD 1,200,000, involving investors referenced in public materials as including Lemniscap and Digital Asset Capital Management (DACM), alongside other participating investors such as Xpring (Ripple), Coil Technologies, 2020 Ventures, Arrington Capital, Hard Yaka, Robot Ventures, UniValues Associates, and additional private investors.

In addition, on or around 29 July 2019, the project is reported to have secured a subsequent venture round, with investors referenced in third-party sources as including HashKey Capital and yield ventures, although the corresponding amount and terms are not consistently disclosed.

Public information further indicates that, in October 2019, Kava conducted an initial exchange offering (IEO) via Binance Launchpad, with an indicated amount of approximately USD 3,000,000 and an indicated token sale price of USD 0.46 per KAVA token.

Further third-party sources also reference, on or around 9 September 2021, an additional large-scale financing event described as an unconfirmed seed round of approximately USD 185,000,000, reportedly intended to support ecosystem growth initiatives. However, this figure is not consistently corroborated across primary sources.

Additional publicly referenced items include portfolio disclosure references (for example, the project being listed as a portfolio company by Arrington XRP Capital Fund LP) and ecosystem-directed allocations such as the establishment of a Kava Strategic Vault (including a reported distribution of 2.5 million AKT from Akash to that vault) as well as a publicly referenced Kava Rise developer incentive program described as a USD 750 million initiative.

However, all such information is derived exclusively from public announcements, portfolio disclosures, press releases, and third-party publications. The issuer, foundation, or entities associated with the KAVA 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

The maximum supply of the crypto-asset is set at 1,080,000,000 tokens. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the

market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

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

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

MiCA-compliant crypto-asset service providers shall have strong measures in place in order to manage conflicts of interests. Due to the broad audience this white paper is addressing, 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) or an asset-referenced token (ART).

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

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

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

F.2 Crypto-asset functionality

According to public information available in the official Kava documentation (https://docs.kava.io/, accessed 2026-03-02), KAVA is the native crypto-asset of the Kava Network and is intended to function as the primary on-chain economic and coordination mechanism within the Kava ecosystem.

The KAVA crypto-asset functions as a technical component within the Kava Network and its associated protocol environment. It is used to support core network operations and interactions at the protocol level. KAVA is used for the payment of transaction fees on the Kava network, including transactions executed across its protocol environment (including the EVM and IBC-related components) and smart-contract interactions, subject to the technical rules and configurations of the protocol. KAVA is also used in connection with staking mechanisms that contribute to network security and validator operations, including the delegation of KAVA to validators, as well as protocol-level slashing conditions applied in the event of validator misbehaviour or failure to meet uptime and related requirements.

In addition, KAVA may be used to participate in protocol-level governance processes, including proposing and voting on changes to protocol parameters and network configuration. Governance-related decisions may relate to the technical operation and evolution of the protocol, including parameters connected to network security and protocol modules. Any governance-related functionalities are limited to the technical operation and evolution of the protocol and do not confer rights related to the ownership, management, or assets of any legal entity.

The KAVA crypto-asset does not confer ownership, profit participation, governance rights in or 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 Kava protocol environment. The actual usability of KAVA depends on factors such as system stability, smart-contract execution,

development progress, governance decisions, and the operational conditions of the Kava Network, which are outside the control of token holders.

F.3 Planned application of functionalities

Future milestones:

- Real World Assets ecosystem launch (Q2 2026): The project described plans to launch a Real World Assets ecosystem and introduce tokenised financial products with transparent accounting.

- Non-USD stablecoin expansion and autonomous agent execution (Q3 2026): The project described plans to expand to non-USD stablecoins (examples referenced include EUR and JPY) and to evolve AI agents toward autonomous execution use cases.

- Fiat onramps and partner distribution expansion (Q4 2026): The project described plans to expand distribution through fiat onramps and partner integrations to enable access to RWA products via credit card purchases.

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 KAVA 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 (New white paper).

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, and is available on multiple networks. The crypto-asset is fungible up to 6 digits after the decimal point on Kava, Ethereum, Binance Beacon Chain, Polygon and Osmosis. 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: "KAVA" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-03-03).

F.8 Website of the issuer

https://www.kava.io/

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

2026-04-09

F.10 Publication date

2026-04-09

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

J5J62BBD7, CTZ6BN3P9, DVKQFFHGX, JJB4VLPTP, Q8FX17M6Q

F.14 Functionally fungible group digital token identifier

2HZXZQLKX

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

The issuer should be 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 claim capable of legal enforcement against the issuer or any third party.

G.2 Exercise of rights and obligations

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

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

G.3 Conditions for modifications of rights and obligations

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no conditions or mechanisms 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 the future offers to the public of crypto-assets were not available at the time of writing this white paper (2026-03-02).

G.5 Issuer retained crypto-assets

According to publicly available information (source: https://x.com/KAVA_CHAIN, accessed 2026-03-02), Kava Labs is described as holding 25.00% of the total KAVA token supply at the time of the Token Generation Event (TGE).

Based on publicly available information indicating a total token supply of 100,000,000 KAVA at the time of the token generation event (TGE), 25.00% would correspond to 25,000,000 KAVA.

Subsequently, the protocol's tokenomics were publicly described as changing in a way that resulted in a materially higher supply level, with public materials referencing a shift that abolished perpetual inflation and set a hard cap of 1,080,000,000 KAVA, alongside a deflationary mechanism (for example, supply reduction via burning). This means the current maximum supply referenced for KAVA is 1,080,000,000 KAVA. However, the 25.00% allocation figure cited above is calculated against the TGE supply of 100,000,000 KAVA, and later changes to overall supply do not, by themselves, allow an independently verifiable conclusion about the current number of tokens attributable to Kava Labs.

Note on independent verifiability

While a "Kava Labs" allocation is referenced in public sources, this allocation cannot be independently verified on the basis of publicly accessible, independently confirmable information, because wallet addresses that would conclusively represent Kava Labs holdings cannot be reliably attributed to a specific legal entity or natural persons using public data alone. Token movements, custody arrangements (including exchange or third-party custody), and treasury management actions may occur without prior notice and may affect observed concentration of holdings and potential governance influence over time.

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 implemented as of 2026-03-02. Nevertheless, it is possible that the owner of the smart-contract(s) has the ability to increase or decrease the token supply in response to changes in demand. Also, it is possible to decrease the circulating supply, by transferring crypto-assets to so called "burn addresses", which are addresses that render the crypto-asset "non-transferable" after sent to those adresses.

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 1,080,000,000 tokens according to public information (Source: https://docs.kava.io/, accessed 2026-03-02). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

This white paper is submitted by Crypto Risk Metrics GmbH, which is established in Germany. 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 the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is implemented on the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

The following applies to Kava:

1. Network protocols

The Kava Network is a decentralised, permissionless Layer 1 blockchain built using the Cosmos SDK. Consensus and peer-to-peer networking are provided by Tendermint Core (BFT Proof-of-Stake), which coordinates validator block proposals and votes to achieve deterministic finality. Interoperability with other Cosmos-SDK networks is supported through the Inter-Blockchain Communication (IBC) protocol, enabling cross-chain message passing and crypto-asset transfers using cryptographic proofs. Kava additionally maintains an EVM-compatible execution environment to support Ethereum-style smart contract interactions, including standard token interfaces (for example ERC-20 and ERC-1155) within the EVM environment.

2. Transaction and address standards

Transactions are defined and processed through a standardised validation pipeline that includes digital signature verification, nonce and sequence checks, gas accounting, and fee deduction prior to execution. Accounts and addresses follow Cosmos-style representations (commonly Bech32-encoded), while the EVM environment supports Ethereum-compatible address formats for interactions with EVM smart contracts. Transactions may include native module actions (for example governance and staking actions) as well as EVM transactions submitted via JSON-RPC endpoints.

3. Blockchain data structure and block standards

Kava separates block ordering and finalisation from deterministic state execution, with Tendermint Core establishing the canonical block sequence and the application layer executing state transitions. Application state is committed to the block header through a cryptographic state root (AppHash) that is produced by the application and included in the block header as part of the consensus commit process. This provides an auditable linkage between the ordered transaction set and the resulting application state.

4. Upgrade and improvement standards

Protocol changes and upgrades are coordinated through on-chain governance processes operated by KAVA stakers and validators. Governance can be used to change parameters and adopt protocol updates, and upgrades are typically executed through coordinated validator software updates at predefined activation points. In addition, Kava supports delegated governance mechanisms that may allow selected committees to enact limited parameter changes within their mandate, subject to the network's governance framework.

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, decentralization, and functionality. Below are some of the key ones:

1. Network Protocols

The crypto-asset follows a decentralized, 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, finalized 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 Binance Beacon Chain:

BNB Beacon Chain has been shut down at block height 385,251,927 since December 3, 2024.

The following applies to Polygon:

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

The following applies to 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.

H.3 Technology used

The crypto-asset in scope is implemented on the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

The following applies to Kava:

1. Decentralised ledger and execution environments

Kava operates as a decentralised, account-based ledger that records transactions in an append-only blockchain structure. The network supports both Cosmos SDK module-based execution and an EVM-compatible environment for smart contract interactions, enabling users and applications to transact through either module messages or EVM transactions depending on the functionality used.

2. Key management

Users control accounts through public and private key pairs. The protocol relies on cryptographic signatures for transaction authorisation, while wallet software and client implementations handle practical key management, including storage of private keys and recovery material.

3. Node operation and data retention

Nodes maintain the ledger state and can be operated in different configurations, including archival setups that retain full historical state and pruning configurations that retain only recent state to reduce storage requirements.

The following applies to Ethereum:

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

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

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

The following applies to Binance Beacon Chain:

BNB Beacon Chain has been shut down at block height 385,251,927 since December 3, 2024.

The following applies to Polygon:

Polygon operates as a decentralized 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 Osmosis:

The platform functions as an automated market maker (AMM) with customizable 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.

H.4 Consensus mechanism

The crypto-asset in scope is implemented on the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

The following applies to Kava:

Kava operates a Proof-of-Stake consensus mechanism based on Tendermint Core, a Byzantine Fault Tolerant (BFT) algorithm designed to provide fast finality and deterministic state replication. Consensus participants are validators selected from a bounded validator set (top 100 by bonded stake). Validators obtain voting power proportional to their bonded KAVA, including KAVA delegated by third parties. Validators participate in block production and consensus by proposing blocks and broadcasting cryptographic votes. Consensus proceeds in rounds. In each round, a designated proposer proposes a block, after which validators participate in two voting phases, pre-vote and pre-commit. A block is finalised and irreversibly committed once more than two-thirds of total validator voting power pre-commits to the same block in the same round. This provides deterministic, immediate finality once included in a committed block (often referred to as 1-block finality). The mechanism is Byzantine fault tolerant in the sense that the network remains safe and consistent provided less than one-third of total voting power is malicious or unavailable. To enforce correct behaviour, the protocol includes slashing conditions for safety and liveness faults, including penalties for double-signing (signing conflicting blocks) and for sustained downtime that undermines validator availability.

The following applies to Ethereum:

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH, 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 finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon

Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

The following applies to Binance Beacon Chain:

BNB Beacon Chain has been shut down at block height 385,251,927 since December 3, 2024.

The following applies to Polygon:

Polygon is a scaling solution for Ethereum that stores and processes transaction data on its own separate chain and regularly submits checkpoints to Ethereum. This type of scaling solution is sometimes referred to as a plasma chain, and is distinct from sidechains, which don't store checkpoints and Layer 2 solutions that store all transaction data on Ethereum in addition to the checkpoints. Here's a detailed explanation of how Polygon achieves consensus:

Core Concepts

1. Proof of Stake (PoS): Validator Selection: Validators on the Polygon network are selected based on the number of POL tokens they have staked. The more tokens are staked, the higher the chance of being selected to validate transactions and produce new blocks. Delegation: Token holders who do not wish to run a validator node can delegate their POL tokens to validators. Delegated tokens also count towards the block production chance of the validator they are delegated to. Delegators receive a share of rewards earned by validators.

Consensus Process

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

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

The following applies to 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 behavior. The system may be exposed to validator collusion or governance capture.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is implemented on the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

The following applies to Kava:

Kava secures its Proof-of-Stake consensus mechanism through a combined system of rewards, fees, and penalties designed to incentivise honest validator performance and aligned delegator participation.

- Incentive mechanisms (rewards): Validators and delegators may receive rewards for participation in block production and consensus. Historically, rewards were funded through inflationary issuance. Following the Kava 15 upgrade, Kava transitioned to a zero-inflation model effective December 31, 2023, meaning no new KAVA is minted as block rewards and reward flows are funded through accumulated transaction fees and, where applicable, allocations from the community pool.

- Staking and bonding: KAVA is bonded to validators as economic collateral. Bonded KAVA is subject to an unbonding period of 21 days. Delegators participate indirectly by delegating KAVA to validators and receiving a pro-rata share of validator rewards, net of validator commission.

- Transaction fees and disposal: Kava applies a gas-based fee model where fees are paid by transaction senders in KAVA and are used to prioritise transactions and deter spam. Fees are distributed to validators and stakers. In addition, protocol module mechanics may apply burning of surplus fees, including through CDP-related surplus mechanisms, which can reduce total supply over time.

- Penalties and slashing: Bonded stake is subject to slashing for protocol violations, including double-signing and sustained downtime. Slashed amounts are burned, directly reducing bonded stake and creating an economic disincentive for safety and liveness faults.

- Governance-related economic effects: On-chain governance includes deposit and veto mechanics intended to discourage spam and malicious proposals. Proposals require a minimum deposit of 1,000 KAVA to enter the voting process, and deposits may be burned if proposals are rejected under defined veto conditions (for example if the NoWithVeto threshold is exceeded).

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 Binance Beacon Chain:

BNB Beacon Chain has been shut down at block height 385,251,927 since December 3, 2024.

The following applies to Polygon:

Incentive Mechanisms

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

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

3. Economic Security: Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions. Bond Requirements: Validators are required to bond a significant amount of 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 decentralized applications (dApps) on Polygon.

The following applies to Osmosis:

The network incentivizes 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 centralization of liquidity or speculative behavior. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

H.6 Use of distributed ledger technology

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

H.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

Trading in the crypto-asset depends on the uninterrupted operation of the trading 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 – such as meme coins or purely speculative tokens – have become worthless. Investors should be aware that this crypto-asset may lose all of its value.

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

Wallet addresses or transactions connected to the crypto-asset may be linked to sanctioned or illicit activity. Regulatory responses to such findings may include transfer restrictions, 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 cryptoasset

KAVA

S.4 Consensus Mechanism

The crypto-asset in scope is implemented on the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

The following applies to Kava:

Kava operates a Proof-of-Stake consensus mechanism based on Tendermint Core, a Byzantine Fault Tolerant (BFT) algorithm designed to provide fast finality and deterministic state replication. Consensus participants are validators selected from a bounded validator set (top 100 by bonded stake). Validators obtain voting power proportional to their bonded KAVA, including KAVA delegated by third parties. Validators participate in block production and consensus by proposing blocks and broadcasting cryptographic votes. Consensus proceeds in rounds. In each round, a designated proposer proposes a block, after which validators participate in two voting phases, pre-vote and pre-commit. A block is finalised and irreversibly committed once more than two-thirds of total validator voting power pre-commits to the same block in the same round. This provides deterministic, immediate finality once included in a committed block (often referred to as 1-block finality). The mechanism is Byzantine fault tolerant in the sense that the network remains safe and consistent provided less than one-third of total voting power is malicious or unavailable. To enforce correct behaviour, the protocol includes slashing conditions for safety and liveness faults, including penalties for double-signing (signing conflicting blocks) and for sustained downtime that undermines validator availability.

The following applies to Ethereum:

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH, 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 finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

The following applies to Binance Beacon Chain:

BNB Beacon Chain has been shut down at block height 385,251,927 since December 3, 2024.

The following applies to Polygon:

Polygon is a scaling solution for Ethereum that stores and processes transaction data on its own separate chain and regularly submits checkpoints to Ethereum. This type of scaling solution is sometimes referred to as a plasma chain, and is distinct from sidechains, which don't store checkpoints and Layer 2 solutions that store all transaction data on Ethereum in addition to the checkpoints. Here's a detailed explanation of how Polygon achieves consensus:

Core Concepts

1. Proof of Stake (PoS): Validator Selection: Validators on the Polygon network are selected based on the number of POL tokens they have staked. The more tokens are staked, the higher the chance of being selected to validate transactions and produce new blocks. Delegation: Token holders who do not wish to run a validator node can delegate their POL tokens to validators. Delegated tokens also count towards the block production chance of the validator they are delegated to. Delegators receive a share of rewards earned by validators.

Consensus Process

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

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

The following applies to 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 behavior. The system may be exposed to validator collusion or governance capture.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is implemented on the Kava (natively), Ethereum, Binance Beacon Chain, Polygon, and Osmosis networks following the standards described below.

The following applies to Kava:

Kava secures its Proof-of-Stake consensus mechanism through a combined system of rewards, fees, and penalties designed to incentivise honest validator performance and aligned delegator participation.

- Incentive mechanisms (rewards): Validators and delegators may receive rewards for participation in block production and consensus. Historically, rewards were funded through inflationary issuance. Following the Kava 15 upgrade, Kava transitioned to a zero-inflation model effective December 31, 2023, meaning no new KAVA is minted as block rewards and reward flows are funded through accumulated transaction fees and, where applicable, allocations from the community pool.

- Staking and bonding: KAVA is bonded to validators as economic collateral. Bonded KAVA is subject to an unbonding period of 21 days. Delegators participate indirectly by delegating KAVA to validators and receiving a pro-rata share of validator rewards, net of validator commission.

- Transaction fees and disposal: Kava applies a gas-based fee model where fees are paid by transaction senders in KAVA and are used to prioritise transactions and deter spam. Fees are distributed to validators and stakers. In addition, protocol module mechanics may apply burning of surplus fees, including through CDP-related surplus mechanisms, which can reduce total supply over time.

- Penalties and slashing: Bonded stake is subject to slashing for protocol violations, including double-signing and sustained downtime. Slashed amounts are burned, directly reducing bonded stake and creating an economic disincentive for safety and liveness faults.

- Governance-related economic effects: On-chain governance includes deposit and veto mechanics intended to discourage spam and malicious proposals. Proposals require a minimum deposit of 1,000 KAVA to enter the voting process, and deposits may be burned if proposals are rejected under defined veto conditions (for example if the NoWithVeto threshold is exceeded).

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 Binance Beacon Chain:

BNB Beacon Chain has been shut down at block height 385,251,927 since December 3, 2024.

The following applies to Polygon:

Incentive Mechanisms

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

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

3. Economic Security: Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions. Bond Requirements: Validators are required to bond a significant amount of 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 decentralized applications (dApps) on Polygon.

The following applies to Osmosis:

The network incentivizes 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 centralization of liquidity or speculative behavior. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

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

2025-03-03

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

2026-03-03

S.8 Energy consumption

236682.93600 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 consumptions, the so called 'bottom-up' approach is being used. The nodes are considered to be the central factor for the energy consumption of the network. These assumptions are made on the basis of empirical findings through the use of public information sites, open-source crawlers and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the client software. The energy consumption of the hardware devices was measured in certified test laboratories. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset in question 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.

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

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

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

S.10 Renewable energy consumption

37.9124101186 %

S.11 Energy intensity

0.00008 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

78.77118 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 incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal energy cost wrt. one more transaction. Ember (2025); Energy Institute - Statistical Review of World Energy (2024) - with major processing by Our World in Data. "Share of electricity generated by renewables - Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from https://ourworldindata.org/grapher/share-electricity-renewables.

S.16 Key GHG sources and methodologies

To determine the GHG Emissions, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal emission wrt. one more transaction. Ember (2025); Energy Institute - Statistical Review of World Energy (2024) - with major processing by Our World in Data. "Carbon intensity of electricity generation - Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from https://ourworldindata.org/grapher/carbon-intensity-electricity Licenced under CC BY 4.0.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.