CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG R1XC4HQT5

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified on 2026-07-29.

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 Floki (FLOKI) referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed on the Ethereum and Binance Smart Chain networks according to the DTI FFG shown in section F.14, as of 2026-07-13. Each deployment has a fixed maximum supply of 10,000,000,000,000 tokens, minted in full at contract creation, so the aggregate maximum supply is 20,000,000,000,000 tokens. The first activity on Ethereum can be viewed on 2022-01-18 (transaction hash: 0x46d76059be13e17d2c6cf8eaee85e1dcd7ea5cc2bceb8b4d648a49dab8ef62be, source: https://etherscan.io/tx/0x46d76059be13e17d2c6cf8eaee85e1dcd7ea5cc2bceb8b4d648a49dab8ef62be, accessed 2026-07-13). The first activity on Binance Smart Chain can be viewed on 2022-01-21 (transaction hash: 0x6871b1b02c1bf26ebd32de256f0681cd6375c2f4e4df5f6408cb7fa6ec7ad860, source: https://bscscan.com/tx/0x6871b1b02c1bf26ebd32de256f0681cd6375c2f4e4df5f6408cb7fa6ec7ad860, accessed 2026-07-13).

Floki is a community-driven Web3 project that began in June 2021 and has since developed into an ecosystem of products spanning decentralised finance, non-fungible tokens (NFTs), gaming and crypto education. The ecosystem comprises products developed under the Floki brand, including Valhalla, a play-to-earn NFT metaverse game; FlokiFi, a suite of decentralised finance products; Floki University, a crypto education platform; and FlokiPlaces, a marketplace for NFTs and merchandise.

Within the Floki Ecosystem, FLOKI is used as a medium of exchange for payments, participation in decentralised finance products, purchases of NFTs and interactions within the Valhalla metaverse game. A transaction tax of 0.3% applies to FLOKI purchases and sales on Ethereum and BNB Smart Chain, the proceeds of which are directed to a project treasury, and several mechanisms permanently remove FLOKI from circulation over time. Publicly available information indicates that FLOKI holders may participate in proposals and voting conducted through the Floki DAO.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

DE-HH

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. This does not prevent the issuer from being sufficiently identifiable in the future. In certain cases, legal entities, organised development teams, or natural persons may take central positions around a crypto-asset project and may therefore be considered relevant for the assessment of the issuer or issuer-like functions. For example, filings in the United States bankruptcy proceedings of FTX Trading Ltd have identified a Georgian limited liability company, Floki Ltd, in connection with the crypto-asset; its registration has since been suspended. Jackie Xu, as a natural person, appears to have a close connection to the crypto-asset, being named as leading its development, and a person known online as "B" has also been named as a strategist connected to the project, alongside Sabre (@SabreEthereum) and MrBrownWhale (@mrbrownwhale), who have been named in advisory and marketing capacities in connection with the project under pseudonyms. Structures such as a development team or similar

organisational arrangements could also be identified. Such persons or structures may therefore be relevant for the assessment of issuer-like functions in relation to the crypto-asset.

B.3 Legal form

Not applicable.

B.4 Registered address

Not applicable.

Not applicable.

Not applicable.

B.5 Head office

Not applicable.

Not applicable.

Not applicable.

B.6 Registration date

Not applicable, as no registered legal-entity issuer has been identified.

B.7 Legal entity identifier

Not applicable, as no registered legal-entity issuer has been identified.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Identity	Function	Business Address
Not applicable	Not applicable	Not applicable

B.11 Business activity

Not applicable.

B.12 Parent company business activity

Not applicable.

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

C.1 Name

Not applicable 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: "FLOKI", Short Name: "FLOKI" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-07-13).

D.2 Crypto-assets name

Long Name: "FLOKI" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-07-13).

D.3 Abbreviation

Short Name: "FLOKI" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-07-13).

D.4 Crypto-asset project description

According to publicly available information (source: docs.floki.com/floki-whitepaper, accessed 2026-07-13), Floki is a community-driven Web3 project that began in June 2021 and has since developed into an ecosystem of products spanning decentralised finance (DeFi), non-fungible tokens (NFTs), gaming and crypto education. The project describes itself as "the people's cryptocurrency."

The Floki ecosystem comprises several products developed under the Floki brand, including Valhalla, a play-to-earn NFT metaverse game; FlokiFi, a suite of decentralised finance products including the FlokiFi Locker for locking and vesting digital assets; Floki University, a crypto education platform; and FlokiPlaces, a marketplace for NFTs and merchandise.

According to the project's documentation, the Floki ecosystem is developed and promoted by contributors operating under the Floki brand. The documentation describes these activities as being coordinated through a decentralised community and funded primarily through a transaction tax applied to FLOKI trading activity and through the project treasury. Within the ecosystem, the FLOKI crypto-asset is intended to facilitate access to, and interaction with, certain products and services, and may also be used in DAO-style community governance processes. It does not represent shares, ownership interests, or any entitlement to the profits of any entity or person associated with the project.

The future development of the project is expected to depend on governance decisions, as well as technical, economic and regulatory factors. Any 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
Floki Ltd	Other person involved in implementation	Kobuleti I Lane, N11, Marneuli, Georgia	Georgia
Block Forge S.R.L.	Other person involved in implementation	San Jose, Costa Rica	Costa Rica
Jackie Xu	Other person involved in implementation	Cannot be found	Cannot be found
B	Other person involved in implementation	Cannot be found	Cannot be found
Sabre	Other person involved in implementation	Cannot be found	Cannot be found
MrBrownWhale	Other person involved in implementation	Cannot be found	Cannot be found

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 FLOKI 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 FLOKI project maintains an official timeline of historical developments through its official website. Future plans are communicated through the project's official documentation, governance proposals and blog publications (sources: https://floki.com/timeline; https://docs.floki.com/floki-whitepaper; https://blog.floki.com, accessed 2026-07-13).

Past milestones:

- Floki DAO upgrade (2022-01-23): The Nottingham upgrade introduced the Floki DAO governance framework, enabling community governance over selected protocol decisions.

- Blacklist functionality permanently removed (2022-03-20): Following a DAO vote, the project's blacklist functionality was permanently renounced.

- FlokiFi Locker launched (2022-07-31): The FlokiFi Locker protocol was introduced, providing digital asset locking services and establishing a protocol revenue source while incorporating a mechanism that uses part of Locker fees to acquire and permanently remove FLOKI tokens from circulation.

- Transaction tax reduction (2023-02-03): Following DAO approval, the transaction tax applicable to FLOKI was reduced from 3% to 0.3%.

- Valhalla bridge token burn (2023-02-09): Approximately 5.1 trillion FLOKI tokens held in the Valhalla bridge were permanently removed from circulation after the bridge was retired for security reasons.

- TokenFi ecosystem launched (2023-10-27): The TokenFi platform and its associated TOKEN crypto-asset were launched, expanding the broader Floki ecosystem into tokenisation-related services.

- Valhalla Chinese testnet release (2024-02-15): A Chinese-language version of the Valhalla metaverse game became available on the opBNB testnet, extending public testing of the game.

- Floki Name Service launched (2024-06-10): The Floki Name Service was introduced on BNB Chain, providing blockchain naming functionality within the ecosystem.

- Floki Debit Card launched (2024-12-09): The Floki Debit Card became available, enabling users to spend supported crypto-assets through participating payment networks.

Future plans, as publicly communicated: the project states an intention to continue expanding the Floki Ecosystem, including further development of the Valhalla metaverse game, the FlokiFi suite of decentralised finance products, Floki University, and the TokenFi tokenisation platform, which is developed under the same brand as a separate crypto-asset. No specific dates have been publicly committed for these developments.

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 FLOKI 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 FLOKI token has not conducted seed, venture capital, private financing or other institutional funding rounds. Publicly available information instead indicates that the project has been developed through a fair-launch model and has relied primarily on transaction tax revenue and treasury resources rather than external fundraising.

According to publicly referenced information, FLOKI was launched without an initial coin offering, private sale or venture capital financing round. Public sources indicate that development of the Floki ecosystem is funded through a 0.3% transaction tax applied to purchases and sales of FLOKI on the Ethereum and BNB Smart Chain networks, together with assets held in the project treasury, including FLOKI, BNB, ETH and stablecoins.

Public sources further indicate that the project maintains treasury assets through publicly disclosed multi-signature wallets on Ethereum and BNB Smart Chain requiring at least three authorised signatories. According to the project, treasury resources are used to fund ecosystem development, exchange listing costs, marketing activities and operational expenses during periods of lower transaction tax revenue. As of 2026-07-13, the publicly disclosed treasury wallets were observed to hold approximately 80,664,033,851 FLOKI across Ethereum and BNB Smart Chain, together with additional holdings of BNB, ETH, stablecoins and other crypto-assets. However, the specific quantity or percentage of the maximum FLOKI supply intended to be maintained within the treasury has not been publicly disclosed. Although the published wallet addresses allow on-chain balances to be observed, the extent to which these wallets represent the entirety of the project's treasury resources cannot be independently verified. Likewise, no publicly disclosed vesting schedule or lock-up arrangement has been identified for treasury-held FLOKI.

The project treasury has sold treasury-held FLOKI to at least one third-party market maker as part of the management of treasury resources. DWF Labs reportedly purchased approximately USD 5,000,000 of FLOKI from the treasury on 2023-05-25 and subsequently committed to purchase approximately USD 10,000,000 of FLOKI over a two-year period commencing on 2024-02-27. These reported treasury transactions are described as treasury asset sales intended to support ecosystem development and market-making activities rather than fundraising rounds. Additional treasury sales to DWF Labs have been referenced in public sources; however, the reported amounts and current execution status are not consistently disclosed and therefore are not included.

According to publicly available information, no publicly disclosed allocation of tokens to founders, team members or external investors subject to vesting has been identified. Public sources further indicate that the entire maximum FLOKI token supply was released at the token generation event.

However, all such information is derived exclusively from public announcements, portfolio disclosures, press releases, transparency reports, and third-party publications. The persons or structures associated with the crypto-asset project, or entities associated with the FLOKI 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 crypto-asset is deployed on two networks. Each deployment has a fixed maximum supply of 10,000,000,000,000 units, minted in full at contract creation, and neither contract permits further units to be created. The aggregate maximum supply across both deployments is therefore 20,000,000,000,000 units.

Units are permanently removed from circulation by transfer to a burn address on each network. As at 2026-07-28, the burn address held 4,458,190,054,103 units on Ethereum and 5,895,407,513,227 units on BNB Smart Chain, giving 10,353,597,567,331 units removed in aggregate and a remaining supply of 9,646,402,432,668 units (sources: https://etherscan.io/token/0xcf0c122c6b73ff809c693db761e7baebe62b6a2e?a=0x000000000000000000000000000000000000dead; https://bscscan.com/token/0xfb5b838b6cfeedc2873ab27866079ac55363d37e?a=0x000000000000000000000000000000000000dead, accessed 2026-07-28). Burning is not implemented at contract level. It results from recurring mechanisms applied to ecosystem revenues and to early unstaking, so the amount removed increases over time and the remaining supply falls accordingly.

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 number of units actually available on the market may therefore differ from the figures stated above.

E.13 Targeted holders

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

E.14 Holder restrictions

Holder restrictions are subject to the rules applicable to the crypto-asset service provider, as well as any additional restrictions that provider may impose.

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

E.36 Involved costs

The costs involved in accessing the trading platform depend on the specific fee structure and terms of the respective crypto-asset service provider. These may include trading fees, deposit or

withdrawal charges, and network-related transaction fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCA) but is neither classified as an electronic money token (EMT) nor an asset-referenced token (ART). It is a digital representation of value that can be stored and transferred using distributed ledger technology (DLT) or similar technology, without embodying or conferring any rights to its holder. The crypto-asset does not aim to maintain a stable value by referencing an official currency, a basket of assets, or any other underlying rights. Instead, its valuation is entirely market-driven, based on supply and demand dynamics, and it is not subject to any stabilisation mechanism. It is neither pegged to any fiat currency nor backed by any external assets, which distinguishes it from EMTs and ARTs. Furthermore, the crypto-asset is not categorised as a financial instrument, deposit, insurance product, pension product, or any other regulated financial product under EU law. It does not grant financial rights, corporate voting rights, or any

contractual claims to its holders, and therefore remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

According to publicly available information (source: docs.floki.com/floki-whitepaper/technology, accessed 2026-07-13), FLOKI is a fungible protocol token issued as an ERC-20 token on Ethereum and also as a BEP-20 token on Binance Smart Chain. Within the Floki Ecosystem, FLOKI functions as a medium of exchange used for payments, participation in decentralised finance products such as the FlokiFi Locker, purchases of NFTs (including through FlokiPlaces), and interactions within the Valhalla metaverse game.

A transaction tax of 0.3% applies to FLOKI purchases and sales on Ethereum and BSC; the proceeds are directed to a project treasury used to fund further development and marketing of the ecosystem. This tax is not applied when FLOKI is transferred between the two networks using the project's cross-chain bridge. Separately, a share of the fees generated by the FlokiFi Locker (reported as 25% of Locker transaction fees) is used to buy and permanently remove FLOKI from circulation, with the remainder directed to the treasury. FLOKI can also be deposited into a staking programme operated in connection with the ecosystem and may be used in DAO-style community governance processes relating to the Floki Ecosystem.

The FLOKI token does not confer ownership, profit participation, governance rights over any related entity in a corporate law sense, or any form of legally enforceable economic entitlement. All functionalities associated with the token are technical in nature and relate exclusively to interactions within the Floki Ecosystem. The actual usability of FLOKI depends on factors including system stability, governance decisions, development progress, and the operational conditions of the Ethereum and Binance Smart Chain networks, which are outside the control of token holders.

F.3 Planned application of functionalities

Future plans, as publicly communicated: the project states an intention to continue expanding the Floki Ecosystem, including further development of the Valhalla metaverse game, the FlokiFi suite of decentralised finance products, Floki University, and the TokenFi tokenisation platform, which is developed under the same brand as a separate crypto-asset. No specific dates have been publicly committed for these developments.

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 FLOKI crypto-asset for its holders.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

The type of submission is NEWT, which stands for "New".

F.6 Crypto-asset characteristics

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

F.7 Commercial name or trading name

Long Name: "FLOKI" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-07-13).

F.8 Website of the issuer

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, no website of a registered legal-entity issuer has been identified.

General information about the underlying project is made publicly available at: https://floki.com/. This website should not be understood as the website of a registered legal-entity issuer within the meaning of Regulation (EU) 2023/1114 (MiCA).

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

2026-08-28

F.10 Publication date

2026-08-28

F.11 Any other services provided by the issuer

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Therefore, no other services provided by a registered legal-entity issuer have been identified.

It cannot be excluded that natural persons, organised development teams, or other structures connected to the crypto-asset project provide or may provide additional services 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

JSB445WQN, MFB10VML7

F.14 Functionally fungible group digital token identifier

R1XC4HQT5

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, no registered legal-entity issuer has been identified for which LEI eligibility could be assessed.

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are of a purely technical or operational nature and do not constitute rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments. Accordingly, holders do not acquire any legally enforceable claim against the issuer of the crypto-asset or any third party.

G.2 Exercise of rights and obligations

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no applicable procedures or conditions for their exercise. Any interaction or functionality that may be available within the project's technical infrastructure – such as participation mechanisms or protocol-level features – serves operational purposes only and does not create, evidence, or constitute any contractual or statutory entitlement.

G.3 Conditions for modifications of rights and obligations

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no conditions or mechanisms for modifying such rights or obligations. Adjustments to the technical protocol, smart contract logic, or related systems may occur in the ordinary course of development or maintenance. Such changes do not alter the legal position of holders, as no contractual rights exist and no rights arise under applicable law or regulation. Holders should not interpret technical updates or governance-related changes as amendments to legally binding entitlements.

G.4 Future public offers

Information on future public offers was not available at the time of writing this white paper (2026-07-13).

G.5 Issuer retained crypto-assets

Based on publicly available information, no identified issuing entity has been confirmed as holding FLOKI tokens for its own account. However, the project has publicly disclosed treasury multi-signature wallets on Ethereum and BNB Smart Chain that are described as holding assets for the benefit of the Floki ecosystem. As at 2026-07-13, these publicly disclosed treasury wallets were observed to hold approximately 80,664,033,851 FLOKI, together with BNB, ETH, stablecoins and other crypto-assets. According to the project's public disclosures, these treasury assets are intended to fund ecosystem development, exchange listing costs, marketing activities and operational expenses. The extent to which the published wallets represent the entirety of the project's treasury resources cannot be independently verified, and no publicly disclosed vesting schedule or lock-up arrangement has been identified for the treasury-held FLOKI.

The treasury wallets can be observed on-chain on Ethereum and BNB Smart Chain through the block explorers at https://etherscan.io/address/0x2b9d5c7f2EAD1A221d771Fb6bb5E35Df04D60AB0 and https://bscscan.com/address/0x17e98a24f992BB7bcd62d6722d714A3C74814B94. A public blockchain address cannot necessarily be assigned to a single person or entity, which limits the ability to determine exact economic influence, ownership or future actions. Changes in the holdings of these project-associated treasury wallets may negatively impact holders of the crypto-asset.

G.6 Utility token classification

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

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

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

G.8 Utility tokens redemption

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

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-07-13.

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

G.13 Supply adjustment mechanisms

Not applicable.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

Any disputes arising in relation to this white paper or the admission to trading may be brought before the competent courts in Hamburg, Germany.

Part H – information on the underlying technology

H.1 Distributed ledger technology (DLT)

The crypto-asset in scope is implemented on the Ethereum and Binance Smart Chain networks following the standards described below.

H.2 Protocols and technical standards

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

The following applies to Ethereum:

The crypto-asset operates on a defined set of protocols and technical standards that are intended to ensure its security, decentralisation, and functionality. Key items are set out below.

1. Network protocols

Ethereum operates as a decentralised, peer-to-peer network. Nodes communicate using the DevP2P networking stack, with RLPx as the encrypted transport layer for peer-to-peer messages.

Transaction ordering and finality are secured through a Proof-of-Stake (PoS) consensus mechanism. Validators on the Beacon Chain propose blocks, attest to them, and finalise them through Casper FFG operating on top of the LMD-GHOST fork-choice rule. Smart contract execution is performed by the Ethereum Virtual Machine (EVM), which interprets EVM bytecode within the gas limits set by the protocol and by the transaction sender.

2. Transaction and address standards

Ethereum addresses are 20-byte identifiers, derived as the last 20 bytes of the Keccak-256 hash of the uncompressed elliptic-curve public key (excluding the 0x04 prefix). They are commonly represented as 40-character hexadecimal strings with a 0x prefix and an optional EIP-55 mixed-case checksum.

The protocol currently supports the following transaction types:

- Type 0: legacy transactions (pre-EIP-1559).

- Type 1: access-list transactions (EIP-2930).

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

- Type 3: blob-carrying transactions (EIP-4844), introduced with the Dencun upgrade on 2024-03-13.

- Type 4: set-code transactions (EIP-7702), introduced with the Pectra upgrade on 2025-05-07, allow externally owned accounts (EOAs) to authorise delegated code execution during transactions, without permanently converting the account into a smart contract. This enables features such as transaction batching, sponsored gas payments and delegated signing.

3. Blockchain data structure and block standards

The Ethereum state consists of accounts (externally owned accounts and smart contracts) together with their associated storage and code, organised in Modified Merkle Patricia Tries to allow efficient verification.

Each block contains:

- a block header, comprising the parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, and the proposer's signature, among other fields;

- the ordered list of transactions, including smart-contract executions and value transfers; and

- blob commitments, where applicable, referring to data published to the data availability layer under EIP-4844.

Block size is not fixed in bytes. It is constrained by a per-block gas limit, which is adjustable within protocol-defined bounds and currently targets approximately 60 million gas following EIP-7935 (Fusaka, activated on 2025-12-03). EIP-7825 (Fusaka) also introduces a per-transaction gas cap of 16,777,216 gas to improve block composability and resilience against denial-of-service patterns.

The data availability layer used by Layer 2 rollups, introduced through EIP-4844, was further developed by EIP-7691 (Pectra, 2025-05-07), which raised the maximum number of blob commitments per block, and by EIP-7594 (Fusaka, 2025-12-03), which introduced Peer Data Availability Sampling (PeerDAS). PeerDAS enables nodes to verify that blob data has been published by sampling small portions of it, rather than downloading every blob in full. Following PeerDAS, Ethereum uses Blob Parameter Only (BPO) forks, introduced by EIP-7892, to adjust blob targets and maxima between major upgrades.

4. Upgrade and improvement standards

Ethereum protocol upgrades are coordinated through the Ethereum Improvement Proposal (EIP) process. EIPs are published openly, reviewed by core developers and the wider community, and bundled into named hard-fork upgrades. The most recent network upgrades are the Pectra upgrade (2025-05-07) and the Fusaka upgrade (2025-12-03). The next named upgrade currently under preparation by the Ethereum core developers is referred to as Glamsterdam.

The following applies to Binance Smart Chain:

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

H.3 Technology used

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

The following applies to Ethereum:

1. Decentralised Ledger: The Ethereum blockchain acts as the decentralised ledger and execution environment for ETH transactions and smart-contract operations, including ERC-20 token transfers, maintaining an append-only record of transfers and account balances to support transparency and verifiable settlement.

2. Account Model: Ethereum uses two account types: externally owned accounts (EOAs), which are controlled through private keys, and contract accounts, which are controlled through deployed smart contract code. Following the Pectra upgrade on 2025-05-07, EOAs can additionally authorise delegated code execution through EIP-7702 transactions without permanently converting the account into smart contracts.

3. Private Key Management: Users must securely store the private keys and recovery material associated with their wallets. Loss or compromise of a private key may result in irreversible loss of access to the associated ETH or ERC-20 token balance.

4. Cryptographic Integrity: Ethereum uses ECDSA over the secp256k1 elliptic curve for key generation and digital signatures on the execution layer. Keccak-256 hashing is used for transaction hashing, state hashing and address derivation. Ethereum addresses are derived from the last 20 bytes of the Keccak-256 hash of the public key. On the consensus layer, BLS (Boneh-Lynn-Shacham) signatures are used to aggregate validator attestations under the Proof-of-Stake consensus mechanism.

The following applies to Binance Smart Chain:

1. BSC-compatible wallets

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

2. Decentralised Ledger

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

3. BEP-20 token standard

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

4. Scalability and transaction efficiency

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

H.4 Consensus mechanism

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

The following applies to Ethereum:

Ethereum uses a Proof-of-Stake (PoS) consensus mechanism introduced with The Merge on 2022-09-15, which replaced the previous Proof-of-Work consensus model. The PoS mechanism is implemented through Gasper, combining Casper-FFG for finality with the LMD-GHOST fork-choice rule for chain selection. Validators participate in consensus by staking ETH through the Beacon Chain. Validators are pseudo-randomly selected to propose new blocks, while other validators attest to the validity of proposed blocks. The network operates using 12-second slots grouped into epochs of 32 slots. Under normal network conditions, finality is typically achieved after two epochs, approximately 12.8 minutes, through Casper-FFG. The LMD-GHOST fork-choice rule determines the canonical chain based on the accumulated weight of validator attestations. Validators that engage in certain malicious behaviour, such as equivocation or contradictory attestations, may be subject to slashing penalties, while offline validators may incur inactivity penalties. Subsequent network

upgrades, including Dencun (2024-03-13), Pectra (2025-05-07) and Fusaka (2025-12-03), introduced protocol changes affecting Ethereum's consensus mechanism and Layer 2 functionality.

The following applies to Binance Smart Chain:

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof-of-Staked-Authority (PoSA), which combines elements of Delegated-Proof-of-Stake (DPoS) and Proof-of-Authority (PoA). This method is intended to support fast block times and low fees while maintaining a level of decentralisation and security.

Core components

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

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

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

Consensus process

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

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

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

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

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

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

H.5 Incentive mechanisms and applicable fees

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

The following applies to Ethereum:

Ethereum's Proof-of-Stake (PoS) mechanism secures the network through validator incentives and protocol-defined penalties. Validators are required to stake ETH in order to participate in block proposal and attestation activities. A minimum of 32 ETH is required to activate a validator. Following the Pectra upgrade on 2025-05-07, EIP-7251 increased the maximum effective balance per validator from 32 ETH to 2,048 ETH. Validators may receive protocol-defined rewards for proposing blocks, attesting to valid blocks and participating in sync committees. Rewards consist of newly issued ETH and transaction-related fees. Transaction fees on Ethereum follow the mechanism introduced by EIP-1559, under which each transaction includes a base fee that is burned at the protocol level and an optional priority fee paid to the validator proposing the relevant block. Validators that engage in certain malicious behaviour, including equivocation or contradictory attestations, may be subject to slashing penalties. Validators that fail to participate correctly in consensus activities may also incur inactivity penalties. These mechanisms are intended to support validator participation and the economic security of the Ethereum network.

The following applies to Binance Smart Chain:

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

Incentive mechanisms

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

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

3. Candidates: BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to

45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information.

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

Fees on the Binance Smart Chain

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

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

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

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

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

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

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

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

Insolvency of counterparties: If a counterparty involved in holding, routing, or settling the crypto-asset becomes insolvent, enters restructuring, or is otherwise subject to resolution measures, assets held or processed by that counterparty may be frozen, become temporarily unavailable, or be recoverable only in part or not at all, which can result in losses for clients whose positions were maintained through that counterparty. This risk applies in particular where client assets are held on an omnibus basis or where segregation is not fully recognised in the counterparty's jurisdiction.

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

Interpretative note for this section: The risk factors set out in this Part I.2 follow the structure of the applicable MiCA white paper template for crypto-assets other than asset-referenced tokens or e-money tokens under Title II of MiCA, including references to issuer-related risks. For the purposes of this Part I.2, references to an "issuer", "issuer-related risks" or similar terms should be read in line

with the definition of "issuer" under MiCA, including any natural or legal person, or other undertaking, that issues crypto-assets.

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, the risk descriptions in this Part I.2 should be understood as referring, as applicable, to any natural persons, legal persons, undertakings, organised development teams, governance arrangements, or other project-related structures that may materially influence the crypto-asset or the related project, to the extent such persons or structures can be identified from available information.

1. Insolvency of the issuer

As with any commercial entity, the issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, or external shocks (e.g. pandemics, armed conflicts). In such a case, ongoing development, support, and governance of the project may cease, potentially affecting the viability and tradability of the crypto-asset.

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

17. Regulatory action risk

The crypto-asset and the products built around it may become the subject of measures by a competent authority. On 2024-01-26 the Hong Kong Securities and Futures Commission placed two products associated with the FLOKI ecosystem, the "Floki Staking Program" and the "TokenFi Staking Program", on its Suspicious Investment Products Alert List. The Commission stated that neither product had been authorised for offering to the Hong Kong public, that each displays the characteristics of a collective investment scheme as defined in the Securities and Futures Ordinance, and that the administrator of the products had not demonstrated to its satisfaction how the advertised annualised return targets of 30% to over 100% could be achieved. The measure was directed at those two staking programmes; the Commission imposed no restriction on dealings in the crypto-asset itself. The project subsequently stated that it had restricted access for users in Hong Kong, added warnings and paused local marketing. The two products remain on the Alert List as at the date of this white paper. Comparable action in other jurisdictions cannot be excluded and may limit the availability of certain functionalities, restrict trading or adversely affect the transferability, liquidity and value of the crypto-asset. (Sources: https://www.sfc.hk/en/Suspicious-Investment-Products/Floki-Staking-Program-and-TokenFi-Staking-Program; https://blog.floki.com/statement-responding-to-hk-sfc-warning-da148338cea0, both accessed 2026-07-13.)

I.4 Project implementation-related risks

As this white paper relates to admission to trading of the crypto-asset, the risk description below reflects general implementation risks typically associated with crypto-asset projects and relevant for the crypto-asset service provider. The party admitting the crypto-asset to trading is not involved in the project's implementation and does not assume responsibility for its governance, funding, or execution.

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

The custody of crypto-assets relies on secure private key management. Loss, theft, or compromise of private keys results in irreversible loss of access. Custodians, trading venues, or wallet providers may be targeted by cyberattacks. Compatibility issues between wallet software and changes to the blockchain protocol (e.g. network upgrades) can further limit user access or the ability to transfer the crypto-asset.

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the crypto-asset

FLOKI

S.4 Consensus Mechanism

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

The following applies to Ethereum:

Ethereum uses a Proof-of-Stake (PoS) consensus mechanism introduced with The Merge on 2022-09-15, which replaced the previous Proof-of-Work consensus model. The PoS mechanism is implemented through Gasper, combining Casper-FFG for finality with the LMD-GHOST fork-choice rule for chain selection. Validators participate in consensus by staking ETH through the Beacon Chain. Validators are pseudo-randomly selected to propose new blocks, while other validators attest

to the validity of proposed blocks. The network operates using 12-second slots grouped into epochs of 32 slots. Under normal network conditions, finality is typically achieved after two epochs, approximately 12.8 minutes, through Casper-FFG. The LMD-GHOST fork-choice rule determines the canonical chain based on the accumulated weight of validator attestations. Validators that engage in certain malicious behaviour, such as equivocation or contradictory attestations, may be subject to slashing penalties, while offline validators may incur inactivity penalties. Subsequent network upgrades, including Dencun (2024-03-13), Pectra (2025-05-07) and Fusaka (2025-12-03), introduced protocol changes affecting Ethereum's consensus mechanism and Layer 2 functionality.

The following applies to Binance Smart Chain:

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof-of-Staked-Authority (PoSA), which combines elements of Delegated-Proof-of-Stake (DPoS) and Proof-of-Authority (PoA). This method is intended to support fast block times and low fees while maintaining a level of decentralisation and security.

Core components

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

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

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

Consensus process

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

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

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

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

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

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

S.5 Incentive Mechanisms and Applicable Fees

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

The following applies to Ethereum:

Ethereum's Proof-of-Stake (PoS) mechanism secures the network through validator incentives and protocol-defined penalties. Validators are required to stake ETH in order to participate in block proposal and attestation activities. A minimum of 32 ETH is required to activate a validator. Following the Pectra upgrade on 2025-05-07, EIP-7251 increased the maximum effective balance per validator from 32 ETH to 2,048 ETH. Validators may receive protocol-defined rewards for proposing blocks, attesting to valid blocks and participating in sync committees. Rewards consist of newly issued ETH and transaction-related fees. Transaction fees on Ethereum follow the mechanism introduced by EIP-1559, under which each transaction includes a base fee that is burned at the protocol level and an optional priority fee paid to the validator proposing the relevant block. Validators that engage in certain malicious behaviour, including equivocation or contradictory attestations, may be subject to slashing penalties. Validators that fail to participate correctly in consensus activities may also incur inactivity penalties. These mechanisms are intended to support validator participation and the economic security of the Ethereum network.

The following applies to Binance Smart Chain:

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

Incentive mechanisms

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

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

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

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

Fees on the Binance Smart Chain

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

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

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

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

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

2025-07-28

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

2026-07-28

S.8 Energy consumption

210.16099 kWh/a

S.9 Energy consumption sources and methodologies

The energy consumption associated with this crypto-asset is aggregated from multiple contributing components, primarily the underlying blockchain network and the execution of token-specific

operations. To determine the energy consumption of a token, the energy consumption of the underlying blockchain network Ethereum and Binance Smart Chain 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

37.9444457108 %

S.11 Energy intensity

0.00001 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.07053 tCO2e/a

S.14 GHG intensity

0.00000 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are determined using public information sites, open-source and in-house-developed crawlers. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal energy consumption with respect to one additional 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]. Underlying sources: Ember, “Yearly Electricity Data Europe”; Ember, “Yearly Electricity Data”; Energy Institute, “Statistical Review of World Energy”. Retrieved from: https://ourworldindata.org/grapher/share-electricity-renewables

S.16 Key GHG sources and methodologies

To determine GHG emissions, the locations of the nodes are determined using public information sites, open-source crawlers, and crawlers developed in-house. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal emission intensity with respect to one additional 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]. Underlying sources: Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: https://ourworldindata.org/grapher/carbon-intensity-electricity. Licensed under CC BY 4.0.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.