

**White paper drafted under the
European Markets in Crypto-
Assets Regulation (EU)
2023/1114 for FFG Q2537P85K**

Preamble

00. Table of Contents

Preamble	2
01. Date of notification	8
02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	8
03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	8
04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114	8
05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114	8
06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114	8
Summary	8
07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114	8
08. Characteristics of the crypto-asset	8
09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	9
10. Key information about the offer to the public or admission to trading	9
Part A – Information about the offeror or the person seeking admission to trading	10
A.1 Name	10
A.2 Legal form	10
A.3 Registered address	10
A.4 Head office	10
A.5 Registration date	10
A.6 Legal entity identifier	10
A.7 Another identifier required pursuant to applicable national law	10
A.8 Contact telephone number	10
A.9 E-mail address	10
A.10 Response time (Days)	10
A.11 Parent company	10
A.12 Members of the management body	11
A.13 Business activity	11
A.14 Parent company business activity	11
A.15 Newly established	11
A.16 Financial condition for the past three years	11
A.17 Financial condition since registration	12

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading	12
B.1 Issuer different from offeror or person seeking admission to trading	12
B.2 Name	12
B.3 Legal form	12
B.4 Registered address	13
B.5 Head office	13
B.6 Registration date	13
B.7 Legal entity identifier	13
B.8 Another identifier required pursuant to applicable national law	13
B.9 Parent company	13
B.10 Members of the management body	13
B.11 Business activity	13
B.12 Parent company business activity	13
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	13
C.1 Name	13
C.2 Legal form	14
C.3 Registered address	14
C.4 Head office	14
C.5 Registration date	14
C.6 Legal entity identifier	14
C.7 Another identifier required pursuant to applicable national law	14
C.8 Parent company	14
C.9 Reason for crypto-Asset white paper Preparation	14
C.10 Members of the Management body	14
C.11 Operator business activity	14
C.12 Parent company business activity	14
C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	14
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	14
Part D – Information about the crypto-asset project	15
D.1 Crypto-asset project name	15
D.2 Crypto-assets name	15
D.3 Abbreviation	15

D.4 Crypto-asset project description	15
D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project	16
D.6 Utility Token Classification	16
D.7 Key Features of Goods/Services for Utility Token Projects	16
D.8 Plans for the token	16
D.9 Resource allocation	17
D.10 Planned use of Collected funds or crypto-Assets	18
Part E – Information about the offer to the public of crypto-assets or their admission to trading	18
E.1 Public offering or admission to trading	18
E.2 Reasons for public offer or admission to trading	18
E.3 Fundraising target	18
E.4 Minimum subscription goals	18
E.5 Maximum subscription goals	18
E.6 Oversubscription acceptance	18
E.7 Oversubscription allocation	18
E.8 Issue price	18
E.9 Official currency or any other crypto-assets determining the issue price	19
E.10 Subscription fee	19
E.11 Offer price determination method	19
E.12 Total number of offered/traded crypto-assets	19
E.13 Targeted holders	19
E.14 Holder restrictions	19
E.15 Reimbursement notice	19
E.16 Refund mechanism	19
E.17 Refund timeline	19
E.18 Offer phases	19
E.19 Early purchase discount	20
E.20 Time-limited offer	20
E.21 Subscription period beginning	20
E.22 Subscription period end	20
E.23 Safeguarding arrangements for offered funds/crypto- Assets	20
E.24 Payment methods for crypto-asset purchase	20
E.25 Value transfer methods for reimbursement	20
E.26 Right of withdrawal	20
E.27 Transfer of purchased crypto-assets	20

E.28 Transfer time schedule	20
E.29 Purchaser's technical requirements	20
E.30 Crypto-asset service provider (CASP) name	21
E.31 CASP identifier	21
E.32 Placement form	21
E.33 Trading platforms name	21
E.34 Trading platforms Market identifier code (MIC)	21
E.35 Trading platforms access	21
E.36 Involved costs	21
E.37 Offer expenses	21
E.38 Conflicts of interest	21
E.39 Applicable law	22
E.40 Competent court	22
Part F – Information about the crypto-assets	22
F.1 Crypto-asset type	22
F.2 Crypto-asset functionality	22
F.3 Planned application of functionalities	23
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	23
F.4 Type of crypto-asset white paper	23
F.5 The type of submission	23
F.6 Crypto-asset characteristics	23
F.7 Commercial name or trading name	24
F.8 Website of the issuer	24
F.9 Starting date of offer to the public or admission to trading	24
F.10 Publication date	24
F.11 Any other services provided by the issuer	24
F.12 Language or languages of the crypto-asset white paper	24
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	24
F.14 Functionally fungible group digital token identifier	24
F.15 Voluntary data flag	24
F.16 Personal data flag	24
F.17 LEI eligibility	24
F.18 Home Member State	24
F.19 Host Member States	25

Part G – Information on the rights and obligations attached to the crypto-assets	25
G.1 Purchaser rights and obligations	25
G.2 Exercise of rights and obligations	25
G.3 Conditions for modifications of rights and obligations	25
G.4 Future public offers	25
G.5 Issuer retained crypto-assets	25
G.6 Utility token classification	26
G.7 Key features of goods/services of utility tokens	26
G.8 Utility tokens redemption	26
G.9 Non-trading request	26
G.10 Crypto-assets purchase or sale modalities	26
G.11 Crypto-assets transfer restrictions	26
G.12 Supply adjustment protocols	26
G.13 Supply adjustment mechanisms	26
G.14 Token value protection schemes	27
G.15 Token value protection schemes description	27
G.16 Compensation schemes	27
G.17 Compensation schemes description	27
G.18 Applicable law	27
G.19 Competent court	27
Part H – information on the underlying technology	27
H.1 Distributed ledger technology (DTL)	27
H.2 Protocols and technical standards	27
H.3 Technology used	30
H.4 Consensus mechanism	31
H.5 Incentive mechanisms and applicable fees	33
H.6 Use of distributed ledger technology	35
H.7 DLT functionality description	35
H.8 Audit	35
H.9 Audit outcome	35
Part I – Information on risks	36
I.1 Offer-related risks	36
I.2 Issuer-related risks	37
I.3 Crypto-assets-related risks	38
I.4 Project implementation-related risks	41
I.5 Technology-related risks	41

I.6 Mitigation measures	43
Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts	43
J.1 Adverse impacts on climate and other environment-related adverse impacts	43
S.1 Name	43
S.2 Relevant legal entity identifier	43
S.3 Name of the crypto-asset	43
S.4 Consensus Mechanism	43
S.5 Incentive Mechanisms and Applicable Fees	45
S.6 Beginning of the period to which the disclosure relates	47
S.7 End of the period to which the disclosure relates	47
S.8 Energy consumption	47
S.9 Energy consumption sources and methodologies	47
S.10 Renewable energy consumption	48
S.11 Energy intensity	48
S.12 Scope 1 DLT GHG emissions – Controlled	48
S.13 Scope 2 DLT GHG emissions – Purchased	48
S.14 GHG intensity	48
S.15 Key energy sources and methodologies	48
S.16 Key GHG sources and methodologies	48

01. Date of notification

This white paper was notified on 2026-04-09.

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 BASED referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed on the Ethereum, Binance Smart Chain and HyperEVM networks according to the DTI FFG shown in section F.14, as of 2026-04-07. The maximum supply of the crypto-asset is 1,000,000,000 tokens. The first activity on Ethereum can be viewed on 2026-01-08 (transaction hash: 0x71554380fb3ccd559c8e267551d665b2afb3e089b469d59541811958f2543af7, source: <https://etherscan.io/tx/0x71554380fb3ccd559c8e267551d665b2afb3e089b469d59541811958f2543af7>, accessed 2026-04-07). The first activity on Binance Smart Chain can be viewed on 2026-03-06 (transaction hash: 0xb331b720011e54341a4bd7465d35080be6d3ab578631e45bd2eca8f0d2f60a5e, source: <https://bscscan.com/tx/0xb331b720011e54341a4bd7465d35080be6d3ab578631e45bd2eca8f0d2f60a5e>, accessed 2026-04-07). The first activity on HyperEVM can be viewed on 2026-01-08 (transaction hash: 0xbfa427c57c19f9a3f9541fc829a8c141a39fdc28e57a146dee034f5a116a320d, source: <https://hyperevmscan.io/tx/0xbfa427c57c19f9a3f9541fc829a8c141a39fdc28e57a146dee034f5a116a320d>, accessed 2026-04-07).

Based One is a project built around a consumer-facing application environment that is designed to combine trading, spending and staking functionalities within a single account structure. According to the available project information, the application is accessible through web, mobile and desktop interfaces and interacts with the Hyperliquid blockchain infrastructure. Its described functionality includes access to spot and perpetual trading interfaces, prediction-market integration, card-based spending functionality with conversion at the point of sale, AI-related product features, and a launchpool environment for project access within the wider ecosystem.

Within this framework, the BASED crypto-asset is used as a technical component of the project environment and is described as the native crypto-asset of the ecosystem. According to the available project information, the crypto-asset is used in connection with staking arrangements, fee-related benefits, access to certain ecosystem features, and card-tier functionality. Project materials further indicate that the crypto-asset may be used in connection with governance-related functions if such functions are introduced by the project.

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 39120077M9TG001FE242.

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

According to the official project documentation (source: <https://litepaper.based.one/>, accessed 2026-04-07), the issuer of the BASED crypto-asset is identified as the Based Foundation. However, the public materials reviewed for the preparation of this white paper do not provide further identifying information about that entity beyond its name. In particular, no registered address, registration number, legal entity identifier, incorporation details, or other verifiable corporate particulars of the Based Foundation were identified in the official documentation reviewed.

B.3 Legal form

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.4 Registered address

Could not be identified during the drafting of this white paper as of 2026-04-07.

Could not be identified during the drafting of this white paper as of 2026-04-07.

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.5 Head office

Could not be identified during the drafting of this white paper as of 2026-04-07.

Could not be identified during the drafting of this white paper as of 2026-04-07.

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.6 Registration date

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.7 Legal entity identifier

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.8 Another identifier required pursuant to applicable national law

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.9 Parent company

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.10 Members of the management body

Identity	Function	Business Address
Cannot be found	Not applicable	Not applicable

B.11 Business activity

Could not be identified during the drafting of this white paper as of 2026-04-07.

B.12 Parent company business activity

Could not be identified during the drafting of this white paper as of 2026-04-07.

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: "Based", Short Name: "BASED" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-07).

D.2 Crypto-assets name

Long Name: "Based" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-07).

D.3 Abbreviation

Short Name: "BASED" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-07).

D.4 Crypto-asset project description

According to public information published in the Based litepaper (source: <https://litepaper.based.one/>, accessed 2026-04-07), the Based project is a crypto-asset initiative centred on the development of a Web3 consumer application designed to combine trading, spending, staking, and other digital-asset related functions within a single user interface. The project is presented as operating on top of the Hyperliquid blockchain infrastructure and as providing access to multiple product features through web, mobile, and desktop environments. Public materials describe the application as supporting spot and perpetual trading across a range of asset categories, card-based spending of digital-asset balances through payment-card infrastructure, access to integrated prediction-market functionality, and a set of AI-related products and services, including inference access and agent-related tools. The project is further presented as seeking to connect on-chain financial activity with broader consumer-facing use cases through a unified application environment.

Within this broader framework, the BASED crypto-asset is described as a functional element of the ecosystem and as interacting with specific platform features and incentive mechanisms. Public materials indicate that holding or staking BASED may be associated with access to certain platform benefits, including rewards, trading-fee discounts, and participation in launch-related ecosystem features. The crypto-asset is also described as forming part of the wider economic design of the project, including user-incentive arrangements and ecosystem participation mechanisms connected to the operation and growth of the application environment.

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

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

Name of person	Type of person	Business address of person	Domicile of company
Based Foundation	Other person involved in implementation	Cannot be found	Cannot be found
Based Technologies Limited	Other person involved in implementation	Cannot be found	British Virgin Islands
Jun Hao Lim	Other person involved in implementation	Cannot be found	Singapore
Edison Lim	Other person involved in implementation	Cannot be found	Singapore

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

There is no formally published multi-year roadmap for the BASED crypto-asset. Based on public information (source: <https://litepaper.based.one/>; accessed 2026-04-07), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Based protocol and the role of the BASED crypto-asset.

Past milestones:

- Series A Funding Round (February 2026): The project raised USD 11.5 million in a funding round led by Pantera Capital.
- Token Generation Event and Partial Community Release (30 March 2026): On 30 March 2026, the BASED token generation event took place and 24% of total supply was released. Public token allocation materials further indicate that 36% of total supply is allocated to community distribution, with part of that allocation distributed after TGE.

Future milestones:

- Season 3 Distribution (May 2026): Final distribution of tokens to Season 3 participants.
- Based AI Commerce Interface Development (date not specified): The project has communicated plans to expand its AI infrastructure into a broader commerce interface intended to translate user instructions into financial execution flows across trading and payments.
- Additional BASED-Related Features (date not specified): Publicly described developments include further staking-related features such as on-ramp and off-ramp fee discounts, AI consumption credits, and a governance framework.

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 BASED 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 BASED token has conducted a Series A funding round involving venture capital and strategic investors. According to publicly referenced information, in or around February 2026, the project is reported to have completed a Series A funding round in the amount of approximately USD 11,500,000. Publicly referenced materials further indicate that Pantera Capital is reported to have acted as lead investor in that financing round. According to the same sources, additional investors reported to have participated in the round include Coinbase Ventures, Wintermute Ventures, Ethena, Hashed, Spartan Group, and Karatage.

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

result, the referenced investment amounts, investor participation, and any implied cumulative funding figures cannot be independently verified and should be considered indicative only.

D.10 Planned use of Collected funds or crypto-Assets

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The maximum supply of the crypto-asset is set at 1,000,000,000 tokens. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

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

E.14 Holder restrictions

Holder restrictions are subject to the rules applicable to the crypto-asset service provider, as well as 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 gas fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

E.37 Offer expenses

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

E.38 Conflicts of interest

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

Crypto Risk Metrics GmbH has established, implemented, and documented comprehensive internal policies and procedures for the identification, prevention, management, and documentation of conflicts of interest in accordance with applicable regulatory requirements. These internal measures

are actively applied within the organisation. For the purposes of this specific assessment and the crypto-asset covered by this white paper, a token-specific review has been conducted by Crypto Risk Metrics GmbH. Based on this individual review, no conflicts of interest relevant to this crypto-asset have been identified at the time of preparation of this white paper.

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

F.2 Crypto-asset functionality

According to publicly available information in the official Based litepaper (<https://litepaper.based.one/>, accessed 2026-04-07), BASED is a crypto-asset associated with the Based One ecosystem and is described there as the protocol token issued by the Based Foundation. The BASED crypto-asset functions as a technical component within the Based ecosystem and its associated product environment. Holding or staking BASED is used to unlock platform-related benefits, including reduced trading and prediction-market fees, card-related benefits, lower on-ramp and off-ramp fees, future launchpool access and airdrops, and agentic AI consumption credits. The litepaper also describes staking-linked functionality in connection with fee-discount tiers and access to card products offered within the ecosystem. In addition, BASED is used in connection with reward and access mechanisms within the broader ecosystem. The documentation states that users may receive cashback in BASED in connection with card usage and that the token is intended to be used for ecosystem incentives and rewards managed by the Based Foundation. Launchpool-related and AI-related use cases are also described as part of the token's intended functionality within the platform environment.

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

F.3 Planned application of functionalities

Future milestones:

- Season 3 Distribution (May 2026): Final distribution of tokens to Season 3 participants.
- Based AI Commerce Interface Development (date not specified): The project has communicated plans to expand its AI infrastructure into a broader commerce interface intended to translate user instructions into financial execution flows across trading and payments.
- Additional BASED-Related Features (date not specified): Publicly described developments include further staking-related features such as on-ramp and off-ramp fee discounts, AI consumption credits, and a governance framework.

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 BASED 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 multiple networks. The crypto-asset is fungible up to 18 digits after the decimal point on Ethereum, Binance Smart Chain and HyperEVM. 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: "Based" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-07).

F.8 Website of the issuer

<https://basedfoundation.com/>

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

2026-05-12

F.10 Publication date

2026-05-12

F.11 Any other services provided by the issuer

No such services are currently known to be provided by the issuer. However, it cannot be excluded that additional services exist or may be offered in the future outside the scope of Regulation (EU) 2023/1114.

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

EN

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

713C8WJPM; Q3H99491J; WSNQSD82H

F.14 Functionally fungible group digital token identifier

Q2537P85K

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-04-07).

G.5 Issuer retained crypto-assets

According to the Based litepaper (source: <https://litepaper.based.one/>, accessed 2026-04-07), a total of 236,400,000 BASED, representing 23.64% of the total supply, was allocated to the "Ecosystem & Rewards" category as of 30 March 2026. According to the token-allocation table published in the litepaper, this allocation is managed by the Based Foundation and reserved for ongoing growth. Based on this publicly available description, these crypto-assets appear to be retained within the project structure for ecosystem development, rewards, and related growth-oriented purposes.

Note: Although the allocation attributed to the Ecosystem & Rewards category is publicly disclosed in the project's tokenomics documentation, the on-chain wallet addresses associated with these holdings cannot be independently linked to specific natural persons. Token transfers, treasury management activities, or other internal reallocations may occur without prior notice and could affect the concentration of holdings or any governance influence associated with these assets.

G.6 Utility token classification

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

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

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

G.8 Utility tokens redemption

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

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-04-07.

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

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 1,000,000,000 tokens according to public information (source: <https://litepaper.based.one/>, accessed 2026-04-07). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

Any disputes arising in relation to this white paper or the admission to trading may 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 that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Binance Smart Chain and HyperEVM. 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.

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

The following applies to Ethereum:

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

1. Network Protocols

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

- Transactions and smart contract execution are secured through Proof-of-Stake (PoS) consensus.
- Validators propose and attest blocks in Ethereum's Beacon Chain, finalised through Casper FFG.
- The Ethereum Virtual Machine (EVM) executes smart contracts using Turing-complete bytecode.

2. Transaction and Address Standards

Crypto-asset address format: 20-byte addresses derived from Keccak-256 hashing of public keys.

Transaction Types:

- Legacy Transactions (pre-EIP-1559)
- Type 0 (Pre-EIP-1559 transactions)
- Type 1 (EIP-2930: Access list transactions)
- Type 2 (EIP-1559: Dynamic fee transactions with base fee burning)

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

3. Blockchain Data Structure & Block Standards

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

Each block contains:

- Block Header: Parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, proposer signature.
- Transactions: Smart contract executions and token transfers.

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

4. Upgrade & Improvement Standards

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

The following applies to 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.

The following applies to HyperEVM:

The crypto-asset is implemented on the HyperEVM, which forms part of the Hyperliquid Layer 1 blockchain rather than a separate chain. The HyperEVM is secured by the same HyperBFT consensus as the rest of the Hyperliquid network and is intended to provide a general-purpose smart contract environment that can interact directly with the broader Hyperliquid state, including HyperCore components.

1. Network architecture and core protocols

The HyperEVM operates as an EVM-compatible execution environment within the Hyperliquid blockchain. It is not architected as an independent network with separate security assumptions. Instead, it shares the validator set and consensus layer of Hyperliquid's HyperBFT system, which allows direct interoperability with the rest of the chain's state.

2. EVM standard and protocol version

The HyperEVM is based on the Ethereum Cancun release, excluding blob functionality. It therefore follows a familiar Ethereum-style execution model for account-based smart contracts, contract calls, gas metering, and transaction submission through JSON-RPC interfaces. EIP-1559 is enabled on the HyperEVM.

3. Block architecture

The HyperEVM uses a dual-block architecture consisting of fast small blocks and slower big blocks. This structure is intended to separate lower-latency execution from larger or more resource-intensive transactions. The Hyperliquid documentation describes this as one of the main differences between the HyperEVM and more conventional EVM deployments.

4. Developer and interface standards

Standard Ethereum tooling can be used for wallet configuration, contract deployment, and transaction broadcasting, subject to HyperEVM-specific implementation details.

5. Data and interoperability standards

The protocol supports direct interaction between HyperEVM applications and HyperCore functionality through built-in system interfaces, including read precompiles and write system contracts. This gives the HyperEVM a technical role closer to an integrated execution layer than to an isolated EVM sidechain.

H.3 Technology used

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

The following applies to Ethereum:

1. Decentralised Ledger: The Ethereum blockchain acts as a decentralised ledger for all token transactions, with the intention to preserve an unalterable record of token transfers and ownership to ensure both transparency and security.
2. Private Key Management: To safeguard their token holdings, users must securely store their wallet's private keys and recovery phrases.
3. Cryptographic Integrity: Ethereum employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers. The Keccak-256 (SHA-3 variant) Hashing Algorithm is used for hashing and address generation. The crypto-asset uses ECDSA with secp256k1 curve for key generation and digital signatures. Next to that, BLS (Boneh-Lynn-Shacham) signatures are used for validator aggregation in PoS.

The following applies to 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.

The following applies to HyperEVM:

1. Decentralised ledger: The Hyperliquid blockchain acts as a decentralised ledger for transactions and state changes associated with the crypto-asset, preserving a synchronised record across participating validator nodes.

2. HyperEVM execution environment: The crypto-asset is implemented within the HyperEVM, an Ethereum-compatible smart contract environment forming part of the Hyperliquid Layer 1 blockchain. The HyperEVM is based on Ethereum Cancun without blobs and supports standard EVM-style contract deployment and execution.

3. Unified chain state: The HyperEVM is not a separate network. It shares security and state integration with HyperCore, which allows applications deployed on the HyperEVM to interact with other native protocol components on the same blockchain.

4. Private key management: Users must securely control the private keys or wallet credentials associated with their addresses in order to authorise transactions and manage holdings of the crypto-asset. This is an operational requirement of the account-based model rather than a token-specific feature.

5. Cryptographic integrity: The HyperEVM relies on standard cryptographic verification and deterministic execution within the Hyperliquid blockchain environment to validate transactions and maintain ledger integrity.

H.4 Consensus mechanism

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

The following applies to Ethereum:

Ethereum's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH, and a validator is randomly selected to propose each new block. Once proposed, the other validators verify the block's integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalisation occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behaviour or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

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.

The following applies to HyperEVM:

The HyperEVM is secured by HyperBFT, the consensus mechanism used by the Hyperliquid Layer 1 blockchain. The HyperEVM does not operate under a separate consensus process. Instead, it inherits security from the same validator-based system that secures the broader Hyperliquid network. HyperBFT is described by Hyperliquid as a variant of HotStuff and is designed to provide low-latency block production and deterministic finality. Validators participate in block production in proportion to the amount of HYPE staked to them, and a quorum exceeding two thirds of total stake is required for commitment of a round. The validator set is supported through staking and delegation of HYPE. Active validators receive rewards in proportion to delegated stake, while lock-up periods and unstaking delays apply to staked positions. Hyperliquid documentation further states that each validator must maintain a 10,000 HYPE self-delegation requirement to become active, that delegations to a validator have a one-day lock-up, and that transfers from staking account to spot account are subject to a seven-day unstaking queue. The documentation also states that there is currently no automatic slashing implemented for general consensus, although the design contemplates penalties and social-layer responses in the event of large-scale attacks or provably malicious conduct.

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

The following applies to Ethereum:

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while

making the crypto-asset's fee structure more predictable and deflationary during high network activity.

The following applies to 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.

The following applies to HyperEVM:

The HyperEVM uses HYPE as the native gas token for transaction execution. According to the Hyperliquid documentation, the HyperEVM implements an EIP-1559 fee model. Under that model, transactions include a base fee and may include a priority fee. The documentation states that base fees are burned in the standard manner by removing them from total EVM supply. Unlike many other EVM-compatible networks, the Hyperliquid documentation also states that priority fees are burned rather than paid to block proposers, reflecting the fact that the HyperEVM is secured through the wider HyperBFT consensus system rather than a separate EVM-specific proposer incentive design.

At network level, validator incentives remain tied to staking of HYPE on the Hyperliquid blockchain. Validators produce blocks and receive rewards in proportion to delegated stake, and delegators may participate in those rewards subject to validator commission arrangements. Hyperliquid states that validators may charge commission to delegators and that staking rewards accrue through the network staking model rather than through HyperEVM transaction tips.

Accordingly, the economic model relevant to the HyperEVM combines two layers: first, transaction execution on the HyperEVM requires payment of gas in HYPE under an EIP-1559-style mechanism; second, the underlying security of the chain is maintained through validator staking and delegation incentives at Hyperliquid network level. This means that fees applicable to users of the HyperEVM arise primarily from gas consumption, while transaction security is supported by protocol-level staking rewards and validator participation across the broader Hyperliquid blockchain.

H.6 Use of distributed ledger technology

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

H.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

The smart contract that defines the crypto-asset's parameters or governs its transfers may contain coding errors or security vulnerabilities. Exploitation of such weaknesses can result in unintended

token minting, permanent loss of funds, or disruption of token functionality. Even after external audits, undetected vulnerabilities may persist due to the immutable nature of deployed code.

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG001FE242

S.3 Name of the crypto-asset

Based

S.4 Consensus Mechanism

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

The following applies to Ethereum:

Ethereum's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH, and a validator is randomly selected to propose each new block. Once proposed, the other validators verify the block's integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalisation occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behaviour or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

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.

The following applies to HyperEVM:

The HyperEVM is secured by HyperBFT, the consensus mechanism used by the Hyperliquid Layer 1 blockchain. The HyperEVM does not operate under a separate consensus process. Instead, it inherits security from the same validator-based system that secures the broader Hyperliquid network. HyperBFT is described by Hyperliquid as a variant of HotStuff and is designed to provide low-latency block production and deterministic finality. Validators participate in block production in proportion to the amount of HYPE staked to them, and a quorum exceeding two thirds of total stake is required for commitment of a round. The validator set is supported through staking and delegation of HYPE. Active validators receive rewards in proportion to delegated stake, while lock-up periods and unstaking delays apply to staked positions. Hyperliquid documentation further states that each validator must maintain a 10,000 HYPE self-delegation requirement to become active, that delegations to a validator have a one-day lock-up, and that transfers from staking account to spot account are subject to a seven-day unstaking queue. The documentation also states that there is currently no automatic slashing implemented for general consensus, although the design contemplates penalties and social-layer responses in the event of large-scale attacks or provably malicious conduct.

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

The following applies to Ethereum:

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid

ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity.

The following applies to 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.

The following applies to HyperEVM:

The HyperEVM uses HYPE as the native gas token for transaction execution. According to the Hyperliquid documentation, the HyperEVM implements an EIP-1559 fee model. Under that model, transactions include a base fee and may include a priority fee. The documentation states that base fees are burned in the standard manner by removing them from total EVM supply. Unlike many other EVM-compatible networks, the Hyperliquid documentation also states that priority fees are burned rather than paid to block proposers, reflecting the fact that the HyperEVM is secured through the wider HyperBFT consensus system rather than a separate EVM-specific proposer incentive design.

At network level, validator incentives remain tied to staking of HYPE on the Hyperliquid blockchain. Validators produce blocks and receive rewards in proportion to delegated stake, and delegators may participate in those rewards subject to validator commission arrangements. Hyperliquid states that validators may charge commission to delegators and that staking rewards accrue through the network staking model rather than through HyperEVM transaction tips.

Accordingly, the economic model relevant to the HyperEVM combines two layers: first, transaction execution on the HyperEVM requires payment of gas in HYPE under an EIP-1559-style mechanism; second, the underlying security of the chain is maintained through validator staking and delegation incentives at Hyperliquid network level. This means that fees applicable to users of the HyperEVM arise primarily from gas consumption, while transaction security is supported by protocol-level staking rewards and validator participation across the broader Hyperliquid blockchain.

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

2025-04-07

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

2026-04-07

S.8 Energy consumption

579.06115 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 networks: Ethereum, Binance Smart Chain and HyperEVM 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

35.7816449123 %

S.11 Energy intensity

0.00009 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO₂e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.19272 tCO₂e/a

S.14 GHG intensity

0.00002 kgCO₂e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivisation structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal energy cost wrt. one more transaction. Ember (2025); Energy Institute - Statistical Review of World Energy (2024) - with major processing by Our World in Data. "Share of electricity generated by renewables - Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from <https://ourworldindata.org/grapher/share-electricity-renewables>.

S.16 Key GHG sources and methodologies

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

calculated as the marginal emission wrt. one more transaction. Ember (2025); Energy Institute - Statistical Review of World Energy (2024) - with major processing by Our World in Data. "Carbon intensity of electricity generation - Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from <https://ourworldindata.org/grapher/carbon-intensity-electricity>. Licensed under CC BY 4.0.

