

**White paper drafted under the
European Markets in Crypto-
Assets Regulation (EU)
2023/1114 for FFG 5RJT6339X**

Preamble

00. Table of Content

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	10
A.13 Business activity	10
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	13
B4. 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	14
C.1 Name	14
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	15
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	15
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	17
D.9 Resource allocation	18
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	19
E.5 Maximum subscription goals	19
E.6 Oversubscription acceptance	19
E.7 Oversubscription allocation	19
E.8 Issue price	19
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	20
E.14 Holder restrictions	20
E.15 Reimbursement notice	20
E.16 Refund mechanism	20
E.17 Refund timeline	20
E.18 Offer phases	20
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	21
E.26 Right of withdrawal	21
E.27 Transfer of purchased crypto-assets	21

E.28 Transfer time schedule	21
E.29 Purchaser's technical requirements	21
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	22
E.37 Offer expenses	22
E.38 Conflicts of interest	22
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	23
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	24
F.4 Type of crypto-asset white paper	24
F.5 The type of submission	24
F.6 Crypto-asset characteristics	24
F.7 Commercial name or trading name	25
F.8 Website of the issuer	25
F.9 Starting date of offer to the public or admission to trading	25
F.10 Publication date	25
F.11 Any other services provided by the issuer	25
F.12 Language or languages of the crypto-asset white paper	25
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	25
F.14 Functionally fungible group digital token identifier	25
F.15 Voluntary data flag	25
F.16 Personal data flag	25
F.17 LEI eligibility	25
F.18 Home Member State	25
F.19 Host Member States	26

Part G – Information on the rights and obligations attached to the crypto-assets	26
G.1 Purchaser rights and obligations	26
G.2 Exercise of rights and obligations	26
G.3 Conditions for modifications of rights and obligations	26
G.4 Future public offers	26
G.5 Issuer retained crypto-assets	27
G.6 Utility token classification	27
G.7 Key features of goods/services of utility tokens	27
G.8 Utility tokens redemption	27
G.9 Non-trading request	27
G.10 Crypto-assets purchase or sale modalities	27
G.11 Crypto-assets transfer restrictions	27
G.12 Supply adjustment protocols	27
G.13 Supply adjustment mechanisms	27
G.14 Token value protection schemes	28
G.15 Token value protection schemes description	28
G.16 Compensation schemes	28
G.17 Compensation schemes description	28
G.18 Applicable law	28
G.19 Competent court	28
Part H – information on the underlying technology	28
H.1 Distributed ledger technology (DLT)	28
H.2 Protocols and technical standards	28
H.3 Technology used	30
H.4 Consensus mechanism	32
H.5 Incentive mechanisms and applicable fees	33
H.6 Use of distributed ledger technology	34
H.7 DLT functionality description	35
H.8 Audit	35
H.9 Audit outcome	35
Part I – Information on risks	35
I.1 Offer-related risks	35
I.2 Issuer-related risks	37
I.3 Crypto-assets-related risks	38
I.4 Project implementation-related risks	40
I.5 Technology-related risks	40

I.6 Mitigation measures	42
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 cryptoasset	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	48
S.7 End of the period to which the disclosure relates	48
S.8 Energy consumption	48
S.9 Energy consumption sources and methodologies	48
S.10 Renewable energy consumption	49
S.11 Energy intensity	49
S.12 Scope 1 DLT GHG emissions – Controlled	49
S.13 Scope 2 DLT GHG emissions – Purchased	49
S.14 GHG intensity	49
S.15 Key energy sources and methodologies	49
S.16 Key GHG sources and methodologies	49

01. Date of notification

This white paper was notified at 2026-01-07.

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 omissions 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 PENDLE referred to in this white paper is a crypto-asset other than e-money tokens (EMTs) or asset-referenced tokens (ARTs). It is issued on the BNB Smart Chain, Ethereum, and Arbitrum networks as of 2025-12-12, according to the DLT FFG shown in Section F.14. The first on-chain activity of the crypto-asset occurred on 2021-04-27 on the Ethereum network (transaction hash: 0x0bacdfc256704f5f8b153d238bb185d42826f148370b91ce4adc46f55f5905b7, source <https://etherscan.io/tx/0x0bacdfc256704f5f8b153d238bb185d42826f148370b91ce4adc46f55f5905b7>, accessed 2025-12-12), on BNB Smart Chain on 2023-06-27 (transaction hash: 0x9d6d449c014495d0e29c43095e8e2d414510be5be65356d54b6d8e3a71fc6b82, source <https://bscscan.com/tx/0x9d6d449c014495d0e29c43095e8e2d414510be5be65356d54b6d8e3a71fc6b82>, accessed 2025-12-12), on Arbitrum on 2023-06-27 (transaction hash: 0xd1cef3b3dcb11b87d651366d25f1087262cd9ac24f3e0597a937cc435fc7f3c, source <https://arbiscan.io/tx/0xd1cef3b3dcb11b87d651366d25f1087262cd9ac24f3e0597a937cc435fc7f3c>, accessed 2025-12-12)

According to publicly available information from the official Pendle documentation and related technical materials (source: <https://docs.pendle.finance/>, accessed 2025-12-12), the crypto-asset project associated with PENDLE concerns the development and operation of the Pendle protocol, a decentralised finance (DeFi) system designed to enable the tokenisation, trading, and management of yield derived from yield-bearing crypto-assets.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

The registered address of Crypto Risk Metrics GmbH is Lange Reihe 73, 20099 Hamburg, Germany, federal state Hamburg.

A.4 Head office

Crypto Risk Metrics GmbH has no head office.

A.5 Registration date

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

A.6 Legal entity identifier

39120077M9TG0O1FE242

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider, which supports regulated entities in the fulfilment of their regulatory requirements. In this regard, Crypto Risk Metrics GmbH, among other services, acts as a data-provider for ESG data according to article 66 (5). Due to the regulations laid out in article 4 (7), 5 (4) and 66 (3) of the 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 around regulatory technology and risk analytics in the context of the MiCAR framework – has been established progressively and can be realistically considered fully operational since approximately 2024.

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

2024 (unaudited): negative EUR 50.891,81

2023 (unaudited): negative EUR 27.665,32

2022: EUR 104.283,00.

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

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

A fundamental repositioning of the company occurred in 2023 and especially in 2024, when the focus shifted toward 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 finalized 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 materialize 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 via Tokens from projects it has worked for and – due to the 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

B.2 Name

The exact corporate structure and the entity responsible for the issuance of the PENDLE token are not clearly and unambiguously disclosed.

Based on publicly available information contained in the Pendle Protocol Terms of Use (<https://docs.pendle.finance/pendle-v2/TermsOfUse>, accessed 2025-12-15), the entity Univerum Innovations Inc., a corporation incorporated under the laws of the Republic of Panama, is identified as the legal operator of the Pendle Protocol. This entity operates the protocol's website and deploys the smart contracts that enable Pendle Protocol activities, including Pendle V2 and Boros. However, Univerum Innovations Inc. explicitly states that it does not act as a clearing house, broker, dealer, custodian, or token issuer, and that tokens generated within the protocol (including PT and YT) are issued by users on a self-directed, non-custodial basis.

In addition, an older Singapore-registered entity, PENDLE PTE. LTD., incorporated on 7 December 2017, is publicly associated with the Pendle brand and ecosystem through its website (<https://www.pendle.finance/>) and business description. This entity is formally registered for management consultancy services and appears to be linked to the Pendle team's operational presence in

Southeast Asia. However, publicly available records do not clearly establish whether this entity is responsible for the issuance, governance, or ongoing management of the PENDLE token.

No public disclosure conclusively identifies which legal entity, if any, qualifies as the issuer of the PENDLE token within the meaning of Regulation (EU) 2023/1114 (MiCAR). This information could not be independently verified. The absence of a clearly identified and verifiable token issuer increases uncertainty regarding accountability, regulatory responsibility, and legal enforceability, and may negatively affect the overall risk profile of the crypto-asset.

B.3 Legal form

Not applicable. No legal person has been publicly identified as the issuer of the PENDLE token. The crypto-asset appears to follow a decentralized, protocol-based model rather than issuance by a formally constituted company or foundation.

B4. Registered address

Not applicable.

Not applicable.

Not applicable.

B.5 Head office

Not applicable.

Not applicable.

Not applicable.

B.6 Registration date

Not applicable.

B.7 Legal entity identifier

Not applicable.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Identity	Function	Business Address
Not applicable	Not applicable	Not applicable

B.11 Business activity

Not applicable.

B.12 Parent company business activity

Not applicable.

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

C.1 Name

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

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-Asset white paper Preparation

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

C.10 Members of the Management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

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

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

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

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

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

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Pendle", Short Name: "PENDLE" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-01-07).

D.2 Crypto-assets name

Long Name: "Pendle" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-12-01).

D.3 Abbreviation

Short Name: "PENDLE" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-12-01).

D.4 Crypto-asset project description

According to publicly available information from the official Pendle documentation and related technical materials (source: <https://docs.pendle.finance/>, accessed 2025-12-12), the crypto-asset project associated with PENDLE concerns the development and operation of the Pendle protocol, a decentralised finance (DeFi) system designed to enable the tokenisation, trading, and management of yield derived from yield-bearing crypto-assets. The protocol was first announced in March 2021 and is implemented as a collection of open-source smart-contract systems deployed on existing distributed-ledger networks, primarily Ethereum and selected Layer-2 scaling solutions. The project is maintained by contributors to the Pendle ecosystem and operates without reliance on a proprietary Layer-1 or Layer-2 blockchain.

The Pendle protocol provides a technical framework that allows yield-bearing assets to be wrapped into a standardised format and separated into principal and yield components, enabling users to engage in yield-related strategies such as fixed-rate exposure, variable-rate exposure, and liquidity provision. Protocol functionality is executed through smart contracts and automated market mechanisms, and its operation depends on the continued availability of the underlying blockchain infrastructure, validator participation on those networks, and ongoing software maintenance.

Within this framework, the PENDLE crypto-asset functions as the native utility and governance token of the Pendle protocol. It is used to support protocol-level governance processes and economic coordination mechanisms. Governance participation is facilitated through a vote-escrow model, whereby holders may lock PENDLE to obtain vePENDLE, which enables voting on incentive allocation parameters and other protocol configuration decisions defined by the system's governance processes. These functions are technical in nature and are subject to the rules embedded in the relevant smart contracts.

The Pendle project does not involve the granting of ownership rights, profit-participation rights, or legally enforceable claims against any issuer, developer, or contributor. The PENDLE crypto-asset does not constitute equity or a claim on assets or revenues. The long-term evolution of the Pendle protocol, including governance mechanisms, incentive structures, and available functionalities, depends on technical development, user adoption, governance outcomes, and external economic and regulatory factors. Any future modifications to the protocol or its features remain subject to change.

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

Type of person	Name of person	Business address of person	Domicile of company
Other person involved in implementation	Univerum Innovations Inc.	Panama, PA – Panamá District (registered office; exact street address not publicly disclosed)	Panama
Other person involved in implementation	PENDLE PTE. LTD.	Singapore, SG – 138 Cecil Street, #12-01A Cecil Court, 069538	Singapore
Other person involved in implementation	TN Lee (also referred to as "TN")	Publicly available sources indicate Panama; domicile could not be independently verified.	Could not be identified.
Other person involved in implementation	Vu Nguyen	Could not be identified.	Could not be identified.
Other person involved in implementation	GT (likely Gregory Tan Yi Feng)	Could not be identified.	Could not be identified.
Other person involved in implementation	YK (likely Loo Yong Khang)	Could not be identified.	Could not be identified.

D.6 Utility Token Classification

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

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

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of

crypto-asset that is only intended to provide access to a good or a service supplied by its issuer". This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or service supplied solely by the issuer.

D.8 Plans for the token

This section provides an overview of the historical developments related to the PENDLE 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. Past developments cannot be assumed to continue, and changes may affect token holders. Sources: <https://medium.com/pendle/liquidity-drop-bootstrapping-details-ea722ef7c36d>, accessed 2025-12-15; <https://medium.com/pendle/pendle-2025-zenith-cf1a91e6e23f>, accessed 2025-12-15; <https://etherscan.io/token/0x808507121b80c02388fad14726482e061b8da827>, accessed 2025-12-15; <https://messari.io/project/pendle/profile>, accessed 2025-12-15; <https://docs.pendle.finance/ProtocolMechanics/Mechanisms/Tokenomics/>, accessed 2025-12-15.

Past milestones:

- PENDLE Token Deployment and Initial Launch Activities (27 April 2021):

Public Pendle launch communications and early distribution mechanics (including the Liquidity Drop Bootstrapping event) were published around 27 April 2021, consistent with public block-explorer data showing the initial on-chain deployment period for the PENDLE ERC-20 token.

- Pendle V2 Launch on Ethereum (29 November 2022):

Pendle V2 launched on Ethereum, introducing the redesigned AMM and the V2 architecture (including SY-based market structure) and the vote-escrow governance model vePENDLE.

- Vesting Completion and Value Accrual Events (September–December 2024):

Public governance materials reference a milestone in September 2024 indicating completion of vesting for team and investor allocations. Separately, Pendle stated that active vePENDLE holders received approximately \$6.1 million in airdrops distributed in December 2024.

Future milestones:

- V2 Core Improvements:

Pendle has communicated intended improvements to V2, including (i) making pool deployment more accessible via the user interface (to support broader permissionless listings), (ii) implementing dynamic fee mechanisms, and (iii) expanding and improving vePENDLE participation flows beyond current weekly voting patterns.

- Citadels (Distribution Expansion):

Pendle has communicated "Citadels" as a roadmap theme intended to expand PT distribution and product reach, including (i) PT offerings for non-EVM ecosystems (e.g., Solana, TON, HYPE), (ii) a KYCed / institution-oriented product concept for regulated market access, and (iii) exploration of structures aligned with Shariah principles for Islamic finance participants.

- Token emissions transition (April 2026 onward):

Public tokenomics materials describe a decreasing weekly emission schedule (with a 1.1% weekly reduction through April 2026) and an intended switch thereafter to a 2% terminal inflation rate per annum for ongoing incentives.

All described future developments represent intended or potential milestones only. They remain dependent on technological feasibility, resource allocation, regulatory considerations, and general project priorities. There is no certainty that these developments will occur, occur as described, or be maintained in the long term. Deviations from the roadmap may occur without prior notice, and changes may negatively affect the usability or relevance of the token.

D.9 Resource allocation

Not applicable – no specific project-level resources beyond the issuer's general operations as described under D.8 have been identified or disclosed. This limits investors' ability to assess the funding and staffing dedicated specifically to this project.

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 total supply of the crypto-asset PENDLE is 281,527,448 units, according to publicly available on-chain data from the Ethereum blockchain (source: Etherscan token contract data at <https://etherscan.io/token/0x808507121b80c02388fad14726482e061b8da827>, accessed 2025-12-15), as of the date of drafting. This figure represents the current total supply recorded on-chain at this point in time and reflects the cumulative outcome of historical emissions under the protocol's tokenomics.

Investors should note that this amount does not constitute a permanently fixed maximum supply. The PENDLE crypto-asset is subject to an ongoing emission framework, under which additional tokens may be issued in the future for liquidity incentives and ecosystem development.

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

E.13 Targeted holders

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

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

The token is intended to be listed on the trading platform operated by Payward Global Solutions LTD ("Kraken"). Access to this platform depends on regional availability and user eligibility under

Kraken's terms and conditions. Investors should consult Kraken's official documentation to determine whether they meet the requirements for account creation and token trading.

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCA) but is neither classified as an electronic money token (EMT) or an asset-referenced token (ART).

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

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

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

F.2 Crypto-asset functionality

According to publicly available information on the official Pendle documentation and related technical materials (source: <https://docs.pendle.finance/>, accessed 2025-12-15), PENDLE is the native crypto-asset of the Pendle Protocol, a decentralised protocol focused on yield trading and liquidity optimisation.

PENDLE is an ERC-20 crypto-asset originally deployed on the Ethereum blockchain on 27 April 2021 under the contract address 0x808507121b80c02388fad14726482e061b8da827. The token is also issued and made available on additional networks, including Ethereum, Binance Smart Chain, and Arbitrum, to support multi-chain protocol deployments. Core governance functionality, including the vote-escrow mechanism (vePENDLE), remains primarily anchored to the Ethereum blockchain.

Within the Pendle protocol, PENDLE serves governance-related and protocol-coordination functions. Users may lock PENDLE to obtain vePENDLE, which is used to participate in protocol-level decision-making related to the allocation of liquidity incentives and to influence the distribution of token emissions across liquidity pools. vePENDLE additionally functions as the technical mechanism through which holders may receive protocol-generated fees and yield-based rewards, derived from swap fees and yield-related protocol charges. These functions relate exclusively to the internal economic coordination of the Pendle protocol and do not constitute ownership or control rights over any legal entity.

PENDLE's role is limited to governance participation, incentive alignment, and liquidity provisioning mechanisms within the protocol environment.

The PENDLE crypto-asset does not confer ownership, profit participation, or legal governance rights over the issuer or any related entity. All functionalities are technical in nature and depend on the continued operation of the Pendle protocol, the correct execution of smart contracts, governance decisions taken via vePENDLE, and the operational conditions of the underlying blockchains on which the token is deployed.

F.3 Planned application of functionalities

Future milestones:

- V2 Core Improvements:

Pendle has communicated intended improvements to V2, including (i) making pool deployment more accessible via the user interface (to support broader permissionless listings), (ii) implementing dynamic fee mechanisms, and (iii) expanding and improving vePENDLE participation flows beyond current weekly voting patterns.

- Citadels (Distribution Expansion):

Pendle has communicated "Citadels" as a roadmap theme intended to expand PT distribution and product reach, including (i) PT offerings for non-EVM ecosystems (e.g., Solana, TON, HYPE), (ii) a KYCed / institution-oriented product concept for regulated market access, and (iii) exploration of structures aligned with Shariah principles for Islamic finance participants.

- Token emissions transition (April 2026 onward):

Public tokenomics materials describe a decreasing weekly emission schedule (with a 1.1% weekly reduction through April 2026) and an intended switch thereafter to a 2% terminal inflation rate per annum for ongoing incentives.

All described future developments represent intended or potential milestones only. They remain dependent on technological feasibility, resource allocation, regulatory considerations, and general project priorities. There is no certainty that these developments will occur, occur as described, or be maintained in the long term. Deviations from the roadmap may occur without prior notice, and changes may negatively affect the usability or relevance of the token.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

The type of submission is NEWT (New white paper).

F.6 Crypto-asset characteristics

The crypto-assets are crypto-assets other than EMTs and ARTs, which are available on the Ethereum, Arbitrum, and BNB Smart Chain blockchains. The crypto-assets are fungible (up to 18 digits after the decimal point), and 281,527,448 units have already been issued. Investors should note that there is no permanently fixed maximum supply. The PENDLE crypto-asset is subject to an ongoing emission framework, under which additional tokens may be issued in the future for liquidity incentives and ecosystem development.

The tokens are a digital representation of value, and have no inherent rights attached as well as no intrinsic utility.

F.7 Commercial name or trading name

Long Name: "Pendle" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2025-12-01).

F.8 Website of the issuer

No formal issuer can be identified for the crypto-asset. Further information regarding the crypto-asset project is available at: <https://www.pendle.finance/>

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

2026-02-05

F.10 Publication date

2026-02-05

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

46P3KPLQX, 6SSGLNPPP, JKMF5L4KM

F.14 Functionally fungible group digital token identifier

5RJT6339X

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

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

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

G.2 Exercise of rights and obligations

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

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

G.3 Conditions for modifications of rights and obligations

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

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

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

G.4 Future public offers

Information on the future offers to the public of crypto-assets were not available at the time of writing this white paper (2025-12-08).

G.5 Issuer retained crypto-assets

As the issuer could not be determined, no information about retained assets by the issuer itself were available at the time of drafting this white paper (2025-12-15).

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

As of 2025-12-15, there are no protocol-level mechanisms that dynamically increase or decrease the token supply in response to market demand. The protocol does not implement discretionary or algorithmic supply adjustments. However, the token follows a predefined emission framework, under which new tokens are issued according to a fixed schedule for incentive purposes. As a result, the protocol does not define a hard maximum supply at the protocol level.

Notwithstanding the above, the circulating supply may decrease if tokens are voluntarily transferred to so-called burn addresses, which are addresses that render the crypto-assets permanently non-transferable once sent.

G.13 Supply adjustment mechanisms

The Pendle protocol does not rely on a traditional block subsidy or continuous protocol-level inflation. Instead, the supply of the PENDLE token is adjusted through a predefined emission schedule used exclusively for incentive distribution. Token emissions are released on a weekly basis and follow a deterministic decay model, with the emission rate gradually decreasing until April 2026.

From May 2026 onwards, the protocol transitions to a fixed terminal inflation rate of approximately 2% per annum, with newly issued tokens dedicated solely to liquidity and ecosystem incentives. The allocation and distribution of these emissions are governed by protocol parameters and vePENDLE-based voting mechanisms. No discretionary or ad hoc minting mechanisms are implemented beyond this predefined framework.

While the total token supply may increase in accordance with the emission schedule, the protocol does not include automated supply expansion or contraction mechanisms comparable to block-reward-based inflation. The circulating supply may nevertheless decrease if tokens are voluntarily transferred to irrecoverable burn addresses, rendering them permanently non-transferable.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

The crypto-asset in scope is implemented on the Ethereum, Arbitrum and BNB Smart Chain network following the standards described below.

H.2 Protocols and technical standards

The crypto asset that is the subject of this white paper is available on the Ethereum, Arbitrum and BNB Smart Chain network.

The following applies to Ethereum:

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

1. Network Protocols

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

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

2. Transaction and Address Standards

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

Transaction Types:

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

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

3. Blockchain Data Structure & Block Standards

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

Each block contains:

- Block Header: Parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, proposer signature.
- Transactions: Smart contract executions and token transfers.
- Block Size: No fixed limit; constrained by the gas limit per block (variable over time). In line with Ethereum's scalability roadmap, Pectra includes EIP-7691, which increases the maximum number of "blobs" (data chunks introduced with EIP-4844) per block. This change significantly boosts the data availability layer used by rollups, supporting cheaper and more efficient Layer 2 scalability.

4. Upgrade & Improvement Standards

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

The following applies to BNB Smart Chain:

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

The following applies to Arbitrum:

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

H.3 Technology used

The crypto asset that is the subject of this white paper is available on the Ethereum, Arbitrum and BNB Smart Chain network.

The following applies to Ethereum:

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

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

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

The following applies to BNB Smart Chain:

1. BSC-Compatible Wallets

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

2. Ledger

BSC maintains its own decentralized 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 Arbitrum:

1. Arbitrum-Compatible Wallets: The tokens are supported by all wallets compatible with the Ethereum Virtual Machine (EVM), such as MetaMask.

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

3. ERC-20 Token Standard: The Arbitrum network supports tokens implemented under the ERC-20 standard, the same as on Ethereum.

4. Arbitrum supports what is called. MultiVM, which is the combination of EVM support and WASM VM support. The latter one being more efficient (lower gas costs) but specific to Arbitrum.

5. Scalability and Transaction Efficiency:

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

H.4 Consensus mechanism

The crypto asset that is the subject of this white paper is available on the Ethereum, Arbitrum and BNB Smart Chain network.

The following applies to Ethereum:

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

The following applies to BNB Smart Chain:

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof of Staked Authority (PoSA), which combines elements of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA). This method ensures fast block times and low fees while maintaining a level of decentralization and security. Core Components 1. Validators (so-called "Cabinet Members"): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network's security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security. 2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security. 3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus

Process 4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes. 5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network. 6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives 7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB. 8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance. 9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

The following applies to Arbitrum:

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

H.5 Incentive mechanisms and applicable fees

The crypto asset that is the subject of this white paper is available on the Ethereum, Arbitrum and BNB Smart Chain network.

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 BNB Smart Chain:

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

Mechanisms 1. Validators: Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks. 2. Delegators: Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network's security and decentralization by choosing reliable validators. 3. Candidates: Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience. 4. Economic Security: Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network. Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets. Fees on the Binance Smart Chain 5. Transaction Fees: Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators. Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet. 6. Block Rewards: Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions. 7. Cross-Chain Fees: Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience. 8. Smart Contract Fees: Deployment and Execution Costs: Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

The following applies to Arbitrum:

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

H.6 Use of distributed ledger technology

No, DLT not operated by the issuer, offeror, a person seeking admission to trading or a third-party acting on the issuer's their behalf.

H.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

The price and tradability of the crypto-asset depend on actual trading activity on the venues to which the service provider is connected, whether centralized exchanges (CEXs) or decentralized

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 favorable price, resulting in slippage.

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

4. Counterparty and service-provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

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, wars). In such a case, ongoing development, support, and governance of the project may cease, potentially affecting the viability and tradability of the crypto-asset.

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

The issuer may depend on third-party providers for certain core functions, such as technology development, marketing, legal advice, or infrastructure. If these partners discontinue their services,

change ownership, or underperform, the issuer's ability to operate the project or maintain investor communication may be impaired. This could disrupt project continuity or undermine market confidence, ultimately affecting the crypto-asset's value.

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the cryptoasset

Pendle

S.4 Consensus Mechanism

Pendle is present on the following networks: Arbitrum, Binance Smart Chain, Ethereum.

Arbitrum is a Layer 2 solution on top of Ethereum that uses Optimistic Rollups to enhance scalability and reduce transaction costs. It assumes that transactions are valid by default and only verifies them if there's a challenge (optimistic).

Core Components:

- Sequencer: Orders transactions and creates batches for processing.
- Bridge: Facilitates asset transfers between Arbitrum and Ethereum.
- Fraud Proofs: Protect against invalid transactions through an interactive verification process.

Verification Process:

1. Transaction Submission: Users submit transactions to the Arbitrum Sequencer, which orders and batches them.
2. State Commitment: These batches are submitted to Ethereum with a state commitment.
3. Challenge Period: Validators have a specific period to challenge the state if they suspect fraud.
4. Dispute Resolution: If a challenge occurs, the dispute is resolved through an iterative process to identify the fraudulent transaction. The final operation is executed on Ethereum to determine the correct state.

5. Rollback and Penalties: If fraud is proven, the state is rolled back, and the dishonest party is penalized.

Security and Efficiency: The combination of the Sequencer, bridge, and interactive fraud proofs ensures that the system remains secure and efficient. By minimizing on-chain data and leveraging off-chain computations, Arbitrum can provide high throughput and low fees.

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

Core Components:

1. Validators (so-called "Cabinet Members"): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network's security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.

2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security.

3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process

4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes.

5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network.

6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives

7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB.

8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance.

9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity.

The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

S.5 Incentive Mechanisms and Applicable Fees

Pendle is present on the following networks: Arbitrum, Binance Smart Chain, Ethereum.

Arbitrum One, a Layer 2 scaling solution for Ethereum, employs several incentive mechanisms to ensure the security and integrity of transactions on its network. The key mechanisms include:

1. Validators and Sequencers:

- Sequencers are responsible for ordering transactions and creating batches that are processed off-chain. They play a critical role in maintaining the efficiency and throughput of the network.

- Validators monitor the sequencers' actions and ensure that transactions are processed correctly. Validators verify the state transitions and ensure that no invalid transactions are included in the batches.

2. Fraud Proofs:

- Assumption of Validity: Transactions processed off-chain are assumed to be valid. This allows for quick transaction finality and high throughput.

- Challenge Period: There is a predefined period during which anyone can challenge the validity of a transaction by submitting a fraud proof. This mechanism acts as a deterrent against malicious behavior.
- Dispute Resolution: If a challenge is raised, an interactive verification process is initiated to pinpoint the exact step where fraud occurred. If the challenge is valid, the fraudulent transaction is reverted, and the dishonest actor is penalized.

3. Economic Incentives:

- Rewards for Honest Behavior: Participants in the network, such as validators and sequencers, are incentivized through rewards for performing their duties honestly and efficiently. These rewards come from transaction fees and potentially other protocol incentives.
- Penalties for Malicious Behavior: Participants who engage in dishonest behavior or submit invalid transactions are penalized. This can include slashing of staked tokens or other forms of economic penalties, which serve to discourage malicious actions.

Fees on the Arbitrum One Blockchain

1. Transaction Fees:

- Layer 2 Fees: Users pay fees for transactions processed on the Layer 2 network. These fees are typically lower than Ethereum mainnet fees due to the reduced computational load on the main chain.
- Arbitrum Transaction Fee: A fee is charged for each transaction processed by the sequencer. This fee covers the cost of processing the transaction and ensuring its inclusion in a batch.

2. L1 Data Fees:

- Posting Batches to Ethereum: Periodically, the state updates from the Layer 2 transactions are posted to the Ethereum mainnet as calldata. This involves a fee, known as the L1 data fee, which accounts for the gas required to publish these state updates on Ethereum.
- Cost Sharing: Because transactions are batched, the fixed costs of posting state updates to Ethereum are spread across multiple transactions, making it more cost-effective for users.

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

Incentive Mechanisms

1. Validators:

- Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards.

- Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks.

2. Delegators:

- Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks.

- Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network's security and decentralization by choosing reliable validators.

3. Candidates:

Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience.

4. Economic Security:

- Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network.

- Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets.

Fees on the Binance Smart Chain

1. Transaction Fees:

- Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators.

- Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.

2. Block Rewards:

Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions.

3. Cross-Chain Fees:

Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience.

4. Smart Contract Fees:

Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

The 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.

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

2025-01-07

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

2026-01-07

S.8 Energy consumption

3819.15849 kWh/a

S.9 Energy consumption sources and methodologies

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

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

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

S.10 Renewable energy consumption

32.2255486008 %

S.11 Energy intensity

0.00006 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

1.27101 tCO2e/a

S.14 GHG intensity

0.00002 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy used in the operation of the network, node locations are determined using public information sources, open-source node crawlers and proprietary crawling tools. Where no sufficient geographic distribution of nodes is available, reference networks with comparable incentive structures and consensus mechanisms are used for approximation. This geolocation data is then merged with publicly available information sourced from Our World in Data, which draws on datasets from Ember (2025) and the Energy Institute – Statistical Review of World Energy (2024). Energy intensity is calculated as the marginal energy cost of processing a single additional transaction on the network.

Source(s): 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 greenhouse gas (GHG) emissions associated with the operation of the network, node locations are determined using public information sources, open-source node crawlers and

proprietary crawling tools. Where no sufficient geographic distribution of nodes is available, reference networks with comparable incentive structures and consensus mechanisms are used for approximation. This geolocation data is then merged with publicly available information sourced from Our World in Data, which draws on datasets from Ember (2025) and the Energy Institute – Statistical Review of World Energy (2024). Carbon intensity is calculated as the marginal emissions associated with processing a single additional transaction on the network.

Source(s): 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.

