

**White paper drafted under the
European Markets in Crypto-
Assets Regulation (EU)
2023/1114 for FFG 1QM2QZQ5N**

Preamble

00. Table of Contents

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

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading	13
B.1 Issuer different from offeror or person seeking admission to trading	13
B.2 Name	13
B.3 Legal form	13
B.4 Registered address	13
B.5 Head office	13
B.6 Registration date	13
B.7 Legal entity identifier	13
B.8 Another identifier required pursuant to applicable national law	13
B.9 Parent company	13
B.10 Members of the management body	13
B.11 Business activity	13
B.12 Parent company business activity	14
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	15
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	17
D.8 Plans for the token	17
D.9 Resource allocation	18
D.10 Planned use of collected funds or crypto-assets	19
Part E – Information about the offer to the public of crypto-assets or their admission to trading	19
E.1 Public offering or admission to trading	19
E.2 Reasons for public offer or admission to trading	19
E.3 Fundraising target	19
E.4 Minimum subscription goals	19
E.5 Maximum subscription goals	19
E.6 Oversubscription acceptance	20
E.7 Oversubscription allocation	20
E.8 Issue price	20
E.9 Official currency or any other crypto-assets determining the issue price	20
E.10 Subscription fee	20
E.11 Offer price determination method	20
E.12 Total number of offered/traded crypto-assets	20
E.13 Targeted holders	21
E.14 Holder restrictions	21
E.15 Reimbursement notice	21
E.16 Refund mechanism	21
E.17 Refund timeline	21
E.18 Offer phases	21
E.19 Early purchase discount	21
E.20 Time-limited offer	21
E.21 Subscription period beginning	21
E.22 Subscription period end	21
E.23 Safeguarding arrangements for offered funds/crypto-assets	21
E.24 Payment methods for crypto-asset purchase	22
E.25 Value transfer methods for reimbursement	22
E.26 Right of withdrawal	22
E.27 Transfer of purchased crypto-assets	22

E.28 Transfer time schedule	22
E.29 Purchaser's technical requirements	22
E.30 Crypto-asset service provider (CASP) name	22
E.31 CASP identifier	22
E.32 Placement form	22
E.33 Trading platforms name	22
E.34 Trading platforms Market identifier code (MIC)	22
E.35 Trading platforms access	22
E.36 Involved costs	23
E.37 Offer expenses	23
E.38 Conflicts of interest	23
E.39 Applicable law	23
E.40 Competent court	23
Part F – Information about the crypto-assets	23
F.1 Crypto-asset type	23
F.2 Crypto-asset functionality	24
F.3 Planned application of functionalities	25
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	25
F.4 Type of crypto-asset white paper	25
F.5 The type of submission	25
F.6 Crypto-asset characteristics	25
F.7 Commercial name or trading name	26
F.8 Website of the issuer	26
F.9 Starting date of offer to the public or admission to trading	26
F.10 Publication date	26
F.11 Any other services provided by the issuer	26
F.12 Language or languages of the crypto-asset white paper	26
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	26
F.14 Functionally fungible group digital token identifier	26
F.15 Voluntary data flag	26
F.16 Personal data flag	26
F.17 LEI eligibility	26
F.18 Home Member State	26
F.19 Host Member States	26

Part G – Information on the rights and obligations attached to the crypto-assets	27
G.1 Purchaser rights and obligations	27
G.2 Exercise of rights and obligations	27
G.3 Conditions for modifications of rights and obligations	27
G.4 Future public offers	27
G.5 Issuer retained crypto-assets	27
G.6 Utility token classification	28
G.7 Key features of goods/services of utility tokens	28
G.8 Utility tokens redemption	28
G.9 Non-trading request	28
G.10 Crypto-assets purchase or sale modalities	28
G.11 Crypto-assets transfer restrictions	28
G.12 Supply adjustment protocols	28
G.13 Supply adjustment mechanisms	28
G.14 Token value protection schemes	29
G.15 Token value protection schemes description	29
G.16 Compensation schemes	29
G.17 Compensation schemes description	29
G.18 Applicable law	29
G.19 Competent court	29
Part H – information on the underlying technology	29
H.1 Distributed ledger technology (DLT)	29
H.2 Protocols and technical standards	29
H.3 Technology used	33
H.4 Consensus mechanism	36
H.5 Incentive mechanisms and applicable fees	38
H.6 Use of distributed ledger technology	42
H.7 DLT functionality description	42
H.8 Audit	42
H.9 Audit outcome	42
Part I – Information on risks	42
I.1 Offer-related risks	42
I.2 Issuer-related risks	44
I.3 Crypto-assets-related risks	45
I.4 Project implementation-related risks	47
I.5 Technology-related risks	48

I.6 Mitigation measures	50
Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts	50
J.1 Adverse impacts on climate and other environment-related adverse impacts	50
S.1 Name	50
S.2 Relevant legal entity identifier	50
S.3 Name of the crypto-asset	50
S.4 Consensus Mechanism	50
S.5 Incentive Mechanisms and Applicable Fees	53
S.6 Beginning of the period to which the disclosure relates	56
S.7 End of the period to which the disclosure relates	57
S.8 Energy consumption	57
S.9 Energy consumption sources and methodologies	57
S.10 Renewable energy consumption	57
S.11 Energy intensity	57
S.12 Scope 1 DLT GHG emissions – Controlled	57
S.13 Scope 2 DLT GHG emissions – Purchased	57
S.14 GHG intensity	57
S.15 Key energy sources and methodologies	57
S.16 Key GHG sources and methodologies	58

01. Date of notification

This white paper was notified on 2026-06-05.

02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114

This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading of the crypto-asset is solely responsible for the content of this crypto-asset white paper.

03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114

This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 of the European Parliament and of the Council and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.

04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114

The crypto-asset referred to in this crypto-asset white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114

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

06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114

The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council or the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

Summary

07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114

Warning: This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto-asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law. This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.

08. Characteristics of the crypto-asset

The crypto-asset BAND referred to in this white paper is a crypto-asset other than EMTs and ARTs and is natively implemented on BandChain and is also deployed on the Osmosis, Fantom (legacy; scheduled for retirement on 30 June 2026), Ethereum, and Binance Smart Chain networks according to the DTI FFG shown in section F.14, as of 2026-05-20. At the initial token creation in 2019, there was an initial supply of 100,000,000 BAND. The maximum supply of BAND is unlimited, and it follows a dynamic inflation model. The first activity on BandChain can be viewed on 2021-09-23 (block hash: EBF114F5293E7F95E5A44E9135D78804F6A1DDE35C7046FA4168B0171629B0FA, source: <https://www.mintscan.io/band/block/1>, accessed 2026-05-20). The first activity on Osmosis can be viewed on 2022-01-25 (channel: OSMOSIS/channel-148 - BAND/channel-83, source: <https://www.mintscan.io/osmosis/relayers/channel-148/band/channel-83>, accessed 2026-05-20). The first activity on Fantom can be viewed on 2021-02-19 (transaction hash: 0xcfe2bc72512c4fd7fdd02297b2cb2bea0b248ba680f7086c2c876cb8d7a2ca41, source: <https://www.oklink.com/fantom/tx/0xcfe2bc72512c4fd7fdd02297b2cb2bea0b248ba680f7086c2c876cb8d7a2ca41>, accessed 2026-05-20). The first activity on Ethereum can be viewed on 2019-09-09 (transaction hash: 0xa74c506c727d2da4bcf8a191a2fc434af408ddbd36b24c2d032dcead8228fd25, source: <https://etherscan.io/tx/0xa74c506c727d2da4bcf8a191a2fc434af408ddbd36b24c2d032dcead8228fd25>, accessed 2026-05-20). The first activity on Binance Smart Chain can be viewed on 2020-09-09 (transaction hash: 0x0b420885f367184d242c61d74e0a6472e9d52e468e7dc3592ab721594219119a, source: <https://bscscan.com/tx/0x0b420885f367184d242c61d74e0a6472e9d52e468e7dc3592ab721594219119a>, accessed 2026-05-20).

The project is a decentralised oracle network designed to provide external data to distributed ledger systems. It operates through its own blockchain, BandChain, which is implemented using the Cosmos SDK and relies on a Byzantine Fault Tolerant Delegated Proof-of-Stake consensus mechanism for block production and validation. The network processes data requests through defined data sources and executable scripts, which coordinate the retrieval and aggregation of data from external interfaces. Validators are selected to fulfil these requests and submit data to the network, where results are aggregated and recorded on-chain. Data produced on BandChain may be verified by external systems through cryptographic proofs and relayed across networks using interoperability mechanisms, including inter-chain communication protocols and bridging frameworks.

The BAND crypto-asset is the native token of the BandChain network and is used to support its operation. It is required for staking by validators participating in consensus and may be delegated by holders to validators. The crypto-asset is used to pay transaction fees and may be used in connection with data request fees within the oracle framework. Holders of staked BAND may participate in protocol governance processes. The protocol incorporates mechanisms under which validator stakes may be reduced in defined circumstances, including in cases of protocol rule violations or failure to perform assigned functions.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

The registered address of Crypto Risk Metrics GmbH is Lange Reihe 73, 20099 Hamburg, Germany,
DE-HH

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

The Legal Entity Identifier (LEI) of Crypto Risk Metrics GmbH is 39120077M9TG001FE242.

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

Band Protocol (also known as World Data Corporation).

B.3 Legal form

Could not be found while drafting this white paper (2026-05-20).

B.4 Registered address

The registered address of Band Protocol is Portcullis Chambers, 4th Floor Ellen Skelton Building, 3076 Sir Francis Drake Highway, Road Town, Tortola,

British Virgin Islands,

VG1110

B.5 Head office

Could not be found while drafting this white paper (2026-05-20).

Could not be found while drafting this white paper (2026-05-20).

Could not be found while drafting this white paper (2026-05-20).

B.6 Registration date

Could not be found while drafting this white paper (2026-05-20).

B.7 Legal entity identifier

Could not be found while drafting this white paper (2026-05-20).

B.8 Another identifier required pursuant to applicable national law

Could not be found while drafting this white paper (2026-05-20).

B.9 Parent company

Could not be found while drafting this white paper (2026-05-20).

B.10 Members of the management body

Identity	Function	Business Address
Could not be found	Could not be found	Could not be found

B.11 Business activity

Could not be found while drafting this white paper (2026-05-20).

B.12 Parent company business activity

Could not be found while drafting this white paper (2026-05-20).

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: "Band", Short Name: "BAND" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-17).

D.2 Crypto-assets name

Long Name: "Band" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-17).

D.3 Abbreviation

Short Name: "BAND" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-17).

D.4 Crypto-asset project description

According to publicly available information (source: <https://docs.bandchain.org/> and related documentation, accessed 2026-05-20), the BandChain ecosystem is a crypto-asset initiative concerned with the development and operation of a decentralised data infrastructure implemented as a sovereign distributed-ledger network within the broader Cosmos ecosystem. The project is designed to facilitate the aggregation and delivery of real-world data to smart contracts and blockchain-based applications across multiple independent networks through the use of interoperable communication standards. BandChain is built using the Cosmos SDK framework and operates as an application-specific blockchain that integrates with other networks via the Inter-Blockchain Communication (IBC) protocol, enabling the transfer of data and assets between compatible chains based on cryptographic verification mechanisms. Within this framework, BandChain functions as a coordination and execution environment for decentralised data provisioning activities, allowing participants to create and interact with oracle infrastructure that sources, aggregates, and delivers price and other real-world data to consuming applications algorithmically. The operation of the network depends on the continued availability and performance of its underlying software components, validator participation, and interoperability with external IBC-enabled networks.

The BandChain network utilises a Delegated Proof-of-Stake (DPoS) consensus mechanism, under which validators are responsible for block production, transaction validation, and oracle data fulfilment. Participants may delegate tokens to validators in order to support network security and participate indirectly in consensus. The protocol also incorporates mechanisms for cross-chain data provisioning, including native Threshold Signature Scheme (TSS) based verification and support for

the IBC standard, enabling consuming applications on multiple connected networks to access and verify data outputs without reliance on centralised intermediaries. Certain features, including oracle sampling parameters, data tunnel configurations, the composition of the TSS group, and price signal prioritisation within the Concurrent Price Stream, depend on governance decisions and technical implementation and may be modified over time.

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

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

Name of person	Type of person	Business address of person	Domicile of company
Chain Lab Co., Ltd.	Other person involved in implementation	Emporium Tower, 24th Floor, Sukhumvit 24, Ban Khlong Tan, Khlong Toei, Bangkok 10110	Thailand
Soravis Srinawakoon	Other person involved in implementation	Emporium Tower, 24th Floor, Sukhumvit 24, Ban Khlong Tan, Khlong Toei, Bangkok 10110	Thailand
Sorawit Suriyakarn	Other person involved in implementation	Emporium Tower, 24th Floor, Sukhumvit 24, Ban Khlong Tan, Khlong Toei, Bangkok 10110	Thailand
Paul Nattapatsiri	Other person involved in implementation	Emporium Tower, 24th Floor, Sukhumvit 24, Ban Khlong Tan, Khlong Toei, Bangkok 10110	Thailand
Band Protocol (also known as World Data Corporation)	Other person involved in implementation	Portcullis Chambers, 4th Floor Ellen Skelton Building, 3076 Sir Francis Drake Highway, Road Town, Tortola, British Virgin Islands VG1110	British Virgin Islands

D.6 Utility Token Classification

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

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

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

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

D.8 Plans for the token

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

There is a formally published roadmap for the BAND crypto-asset and the Band protocol. Based on the official roadmap (source: <https://blog.bandprotocol.com/band-protocol-is-now-band/>; accessed 2026-05-20), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Band protocol and the role of the BAND crypto-asset.

Past milestones:

- Data Delivery Commencement (2018): The Band protocol began delivering price data to the Web3 ecosystem, establishing its foundational role as an oracle data provider.
- Initial Exchange Offering on Binance Launchpad (2019-09-17): The project completed its Initial Exchange Offering on Binance Launchpad, raising USD 5.85 million in connection with the public distribution of the BAND crypto-asset.
- Migration to BandChain (2020): The project migrated from an Ethereum-based token infrastructure to a dedicated Cosmos-SDK blockchain, BandChain, marking a significant change to the technical architecture underlying the BAND crypto-asset.
- GuanYu Mainnet Launch (October 2020): The GuanYu mainnet was launched, enabling the permissionless creation of customisable data oracle scripts and expanding the programmable features of the protocol.
- Band Protocol v3 Mainnet Launch (2025-07-09): Band Protocol v3 was officially launched on mainnet, introducing a modular framework architecture and one-second feed update intervals, representing a material upgrade to the protocol's data delivery capabilities.

- Rebranding to Band (2025-08-04): The project rebranded from Band Protocol to Band, repositioning the protocol as a data layer for both Web3 and artificial intelligence applications.

Future milestones:

- Expansion to Multi-Chain Ecosystem (2026 and beyond): The protocol intends to expand Band v3 into a broader multi-chain ecosystem, increasing the number of supported blockchain networks and the scope of data availability.
- Global Data Availability with Privacy and Composability (2026 and beyond): The project's published roadmap indicates an objective to achieve global data availability with a focus on privacy and composability, aimed at supporting both autonomous systems and financial protocols.
- Integration with Large Language Model Infrastructure (2026 and beyond): The protocol plans to establish integrations with large language model infrastructure, with the stated purpose of enabling data contributions to be used within artificial intelligence applications.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the BAND crypto-asset for its holders.

D.9 Resource allocation

Based on information from various third-party and industry sources, it is reported that the crypto-asset project associated with the BAND token has conducted multiple funding rounds involving venture capital investment, private token sales, and a public initial exchange offering, collectively raising a reported total of approximately USD 10.85 million in its early stages.

According to publicly referenced information, the project's first identifiable institutional financing round took place in 2019, when Band Protocol is reported to have raised approximately USD 3,000,000 from a group of venture capital investors. Public sources identify the India unit of Sequoia Capital as a primary participant in this round, though the precise terms, valuation, and full composition of the investor syndicate have not been independently disclosed.

Public sources further indicate that, in addition to the institutional round described above, Band Protocol conducted private token sales during the same period, raising a further reported amount of approximately USD 2,000,000 from early investors. The identity of those investors and the contractual basis of the private sales have not been confirmed through independent disclosure.

Further public reporting indicates that, on 17 September 2019, Band Protocol completed an initial exchange offering on the Binance Launchpad platform. Third-party reporting describes the gross proceeds of this public sale as approximately USD 5,850,000, equivalent to approximately 282,207

BNB at the time of the offering. This event is reported as representing the principal public financing event in the project's early history.

No further institutional financing rounds, ecosystem grants, treasury allocations, or formally disclosed incentive programmes have been identified in publicly available sources at the time of preparation of this white paper.

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

D.10 Planned use of collected funds or crypto-assets

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

As of 2026-05-20, the total supply of BAND was approximately 176,530,710 BAND, according to publicly available information. BAND does not have a fixed maximum supply. At the initial token creation in 2019, an initial supply of 100,000,000 BAND was created and allocated across the following categories, according to publicly available information:

- Ecosystem: 25.63%
- Team and Advisors: 25%
- Foundation: 22%
- Investors: 15%
- Public Sale (IEO): 12.37%

The supply of BAND has changed since the protocol's launch and may continue to change through protocol-defined mechanisms. BandChain operates an inflationary issuance model targeting a staking ratio of approximately 66% of total supply, with the annual inflation rate adjusting between 7% and 20% (according to the BandChain documentation at docs.bandchain.org, accessed 2026-05-21). Newly issued BAND is allocated at each block to validators and delegators participating in the network's Delegated Proof-of-Stake consensus.

Holders of BAND should note that increases in total supply through inflationary issuance, and any future protocol-defined changes to issuance or supply mechanics, may affect the proportion of total

supply represented by their holdings. The circulating supply may differ from the total supply at any given time.

E.13 Targeted holders

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

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

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

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCA) but is neither classified as an electronic money token (EMT) nor an asset-referenced token (ART). It is a digital representation of value that can be stored and transferred using distributed ledger technology (DLT) or similar technology, without embodying or conferring any rights to its holder. The crypto-asset does not aim to maintain a stable value by

referencing an official currency, a basket of assets, or any other underlying rights. Instead, its valuation is entirely market-driven, based on supply and demand dynamics, and it is not subject to any stabilisation mechanism. It is neither pegged to any fiat currency nor backed by any external assets, which distinguishes it from EMTs and ARTs. Furthermore, the crypto-asset is not categorised as a financial instrument, deposit, insurance product, pension product, or any other regulated financial product under EU law. It does not grant financial rights, voting rights, or any contractual claims to its holders, and therefore remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

According to publicly available information (source: <https://docs.bandchain.org/> and related documentation, accessed 2026-05-20), the BAND token is the native on-chain crypto-asset of the BandChain network and is used for protocol-level participation in network security, oracle data coordination, and on-chain governance. BAND holders can delegate (stake) BAND to validators to support the operation and security of the network and, in return, participate in the distribution of protocol-defined rewards.

BAND's core functionality is based on staking and oracle data coordination within a decentralised data infrastructure environment. The BandChain network maintains an active validator set determined by the quantity of BAND staked to each candidate. Following Band v3 and the Band Active Validators Set introduced under BCIP-17 (2025), the active set has been curated to a smaller group of top-performing validators (most recently reported as 53), within the Cosmos-SDK protocol maximum. In parallel, the protocol facilitates decentralised data provisioning through oracle mechanisms, allowing validators to source, aggregate, and deliver real-world data to consuming applications and to receive incentives based on their participation in data fulfilment and network configuration.

BAND also enables decentralised decision-making through on-chain governance. Bonded BAND holders may submit, deposit on, and vote on governance proposals, including protocol upgrades, parameter adjustments, and the composition or transition of the official Threshold Signature Scheme (TSS) group responsible for cryptographic data verification. Voting power is generally proportional to the amount of bonded BAND, subject to protocol rules and delegation structures.

Within the BandChain network, BAND is used as the accounting basis for validator and delegator incentives as well as for oracle-related reward mechanisms. Incentives may include newly issued BAND distributed to validators and delegators in accordance with a variable inflation model targeting a staking ratio of approximately 66% of total supply, with an annual inflation rate that adjusts between 7% and 20%, as well as transaction-related fees generated through on-chain activity. BAND is additionally used to pay for computational resources (gas) required for on-chain transactions and, where applicable, for fees associated with access to premium data sources.

The BAND token does not confer ownership, profit participation, governance rights over the issuer or any related entity, or any form of economic entitlement. All functionalities are technical in nature and relate exclusively to interactions within the BandChain protocol environment. The actual usability of BAND depends on factors such as system stability, oracle execution, development progress, governance decisions, and the operational conditions of the BandChain blockchain, which are outside the control of token holders.

F.3 Planned application of functionalities

Future milestones:

- Expansion to Multi-Chain Ecosystem (2026 and beyond): The protocol intends to expand Band v3 into a broader multi-chain ecosystem, increasing the number of supported blockchain networks and the scope of data availability.
- Global Data Availability with Privacy and Composability (2026 and beyond): The project's published roadmap indicates an objective to achieve global data availability with a focus on privacy and composability, aimed at supporting both autonomous systems and financial protocols.
- Integration with Large Language Model Infrastructure (2026 and beyond): The protocol plans to establish integrations with large language model infrastructure, with the stated purpose of enabling data contributions to be used within artificial intelligence applications.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the BAND crypto-asset for its holders.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs and is available on the BandChain (native), Osmosis, Fantom (legacy; scheduled for retirement on 30 June 2026), Ethereum, and Binance Smart Chain networks. The crypto-asset is fungible up to 18 decimal places on Fantom, Ethereum, and Binance Smart Chain, and up to 6 decimal places on BandChain and Osmosis. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics such as supply, demand, and liquidity in secondary markets.

F.7 Commercial name or trading name

Long Name: "Band" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-17).

F.8 Website of the issuer

<https://www.bandprotocol.com/>

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

2026-07-07

F.10 Publication date

2026-07-07

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

45J3BLQQC, D1MPWZP6C, WZV5DWB8, VWMZRF3S6, NXRTM7Q1K

F.14 Functionally fungible group digital token identifier

1QM2QZQ5N

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on the future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-05-20).

G.5 Issuer retained crypto-assets

Based on a review of publicly available information, Band Protocol had an initial supply of 100,000,000 BAND tokens at genesis. Of this initial supply, 22% was allocated to the Foundation, corresponding to 22,000,000 BAND. These tokens were allocated in connection with the initial distribution of BAND and were intended to support the long-term development, oversight and ecosystem-related activities of the Band Protocol.

For the purposes of this section, the 22,000,000 BAND allocated to the Foundation may be considered retained crypto-assets, to the extent that they were held or controlled, directly or indirectly, by an entity associated with the development and support of the Band Protocol ecosystem at the time of the initial distribution.

It should be noted that BAND does not have a fixed maximum supply. The initial supply of 100,000,000 BAND reflects the supply at genesis and does not represent a permanent supply cap. The Band Protocol applies an inflationary model under which additional BAND may be issued over

time as part of the protocol's staking and network incentive mechanisms. As a result, the Foundation allocation represented 22% of the initial genesis supply, but this percentage may not correspond to the same proportion of the total supply at later points in time.

No publicly verifiable blockchain addresses have been identified as being attributable to the Foundation treasury holdings. As a result, it is not possible to independently confirm, via on-chain analysis, the exact quantity, location, or current status of such crypto-assets. Accordingly, the information presented in this section should be understood as an indicative statement based on available historical token distribution information, and not as a definitive or independently verifiable statement of current retained crypto-assets.

G.6 Utility token classification

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

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

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

G.8 Utility tokens redemption

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

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-05-20.

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

G.13 Supply adjustment mechanisms

Not applicable.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DLT)

The crypto-asset in scope is implemented natively on BandChain and is also deployed on the Osmosis, Fantom (legacy; scheduled for retirement on 30 June 2026), Ethereum, and Binance Smart Chain networks, following the standards described below.

H.2 Protocols and technical standards

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

The following applies to BandChain:

1. Network Protocols

The BandChain network operates on a modular and decentralised architecture based on the Cosmos SDK framework. Consensus and peer-to-peer networking are provided by Tendermint

Core, a Byzantine Fault Tolerant consensus engine designed to enable deterministic state replication and fast finality. Cross-chain interoperability is supported through the Inter-Blockchain Communication (IBC) protocol, which enables BandChain to transmit verified data across compatible blockchain networks. In addition, BandChain incorporates a Threshold Signature Scheme (TSS) module to facilitate secure cross-chain data verification through distributed key management and collective signing. The protocol rules governing network operation are defined through structured specifications, including Protocol Buffers (Protobuf) for message and state definitions, as well as application-specific execution logic implemented through Oracle WebAssembly (Owasm).

2. Transaction and Address Standards

Transactions on BandChain are defined through Cosmos SDK message types and follow a standardised validation pipeline that includes signature verification, fee validation, and execution of application-level logic. Accounts are identified by addresses derived from public keys using the BIP44 hierarchical deterministic wallet standard and encoded using Bech32 format. Transactions may include operations such as token transfers, staking actions, and oracle data requests (e.g., `MsgRequestData`, `MsgReportData`). Transaction fees are applied to prevent resource abuse and are typically paid by the transaction sender. Additional fees may apply for specific oracle data requests depending on the underlying data source.

3. Blockchain Data Structure & Block Standards

BandChain separates consensus from application-level execution. Tendermint is responsible for ordering and finalising blocks, while the application layer executes deterministic state transitions. Application state is maintained using Merkle-based data structures, specifically iAVL trees, which allow efficient verification of stored data through Merkle proofs. The resulting state root is committed to each block header and validated by a supermajority of validators. Oracle-related data is stored within a dedicated application state structure (oracle store), where results are permanently recorded and can be verified by external systems using light client protocols.

4. Upgrade & Improvement Standards

Protocol upgrades and parameter changes are coordinated through on-chain governance mechanisms. Network participants may submit and vote on proposals that modify protocol behaviour, including validator parameters, oracle configurations, or system modules. Certain protocol components, such as the Threshold Signature Scheme group, may be updated through governance messages (e.g., group transition proposals). Validators are required to adopt updated software versions at specified upgrade points to maintain network compatibility and continuity.

The following applies to Osmosis:

1. Network Protocols

Osmosis is an application-specific Layer 1 blockchain built using the Cosmos SDK. Consensus and peer-to-peer networking are provided through CometBFT, formerly Tendermint Core, which implements Byzantine Fault Tolerant state-machine replication. Osmosis also supports cross-chain

communication through the Inter-Blockchain Communication protocol, which enables transfers and messages between IBC-enabled chains.

2. Transaction and Address Standards

Transactions are processed through Cosmos SDK modules and may include transfers, swaps, staking, governance actions, and IBC transfers. Osmosis uses Cosmos-style account and transaction standards, including Bech32-format addresses and sequence-based account handling. IBC transfers follow the ICS-20 fungible token transfer standard.

3. Blockchain Data Structure & Block Standards

Osmosis separates consensus from application-level execution. CometBFT orders and finalises blocks, while the Osmosis application layer executes deterministic state transitions through Cosmos SDK modules. Application state is committed through cryptographic state roots included in block headers, allowing validators to agree on the resulting network state.

4. Upgrade & Improvement Standards

Protocol upgrades are coordinated through Osmosis governance and scheduled software upgrades. Validators are required to run compatible software at the relevant upgrade point. As an IBC-connected chain, Osmosis upgrades

must also preserve compatibility with IBC clients, channels, and counterparty chains where applicable.

The following applies to Fantom:

Since the migration from the Fantom ecosystem to the Sonic ecosystem is ongoing, the Fantom Opera network should be understood as legacy infrastructure, while the Sonic network represents the successor network and the primary focus of ongoing ecosystem development. Fantom Opera continues to exist during a transitional period; however, Sonic Labs has announced that remaining legacy Opera infrastructure, including the Opera FTM-to-S bridge, is expected to be retired on 30 June 2026 at 17:00 GMT. Historical chain data is expected to remain preserved, while future technical development and operational focus are directed towards Sonic.

The following applies to Ethereum:

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

1. Network protocols

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

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

2. Transaction and address standards

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

The protocol currently supports the following transaction types:

- Type 0: legacy transactions (pre-EIP-1559).
- Type 1: access-list transactions (EIP-2930).
- Type 2: dynamic-fee transactions with base-fee burning (EIP-1559).
- Type 3: blob-carrying transactions (EIP-4844), introduced with the Dencun upgrade on 2024-03-13.
- Type 4: set-code transactions (EIP-7702), introduced with the Pectra upgrade on 2025-05-07, allow externally owned accounts (EOAs) to authorise delegated code execution during transactions, without permanently converting the account into a smart contract. This enables features such as transaction batching, sponsored gas payments and delegated signing.

3. Blockchain data structure and block standards

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

Each block contains:

- a block header, comprising the parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, and the proposer's signature, among other fields;
- the ordered list of transactions, including smart-contract executions and value transfers; and
- blob commitments, where applicable, referring to data published to the data availability layer under EIP-4844.

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

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

4. Upgrade and improvement standards

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

The following applies to Binance Smart Chain:

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

H.3 Technology used

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

The following applies to BandChain:

1. Decentralised Ledger

BandChain operates as a decentralised, account-based ledger that records transactions in an append-only blockchain structure. Blocks are validated and finalised through a Byzantine Fault Tolerant consensus mechanism, ensuring that recorded oracle data, token transfers, and state changes are consistently replicated across the network.

2. Private Key Management

Users are responsible for the secure storage and management of private keys associated with their accounts. The BandChain protocol does not prescribe specific custody solutions. Key management is handled at the wallet or client level, including software and hardware wallets compatible with Cosmos SDK standards.

3. Modular Design and Smart Contracting

BandChain follows a modular architecture based on the Cosmos SDK. Core functionality includes oracle data request handling, aggregation logic, and staking mechanisms implemented at the application layer. Custom logic for oracle data processing is implemented through Oracle WebAssembly (Owasm), a domain-specific execution environment based on WebAssembly. Oracle scripts define how external data is requested, validated, and aggregated into final on-chain results. The execution model typically follows a two-phase process involving data request specification and subsequent aggregation of validator-provided responses into a single deterministic output.

The following applies to Osmosis:

1. Decentralised Ledger

Osmosis operates as a decentralised ledger that records all transactions in an append-only blockchain structure. Blocks are validated and finalised through a Byzantine Fault Tolerant consensus mechanism, with the intention of preserving an unalterable and transparent record of token transfers, liquidity pool interactions, and balances.

2. Private Key Management

To safeguard their OSMO holdings, users must securely store their wallet private keys and recovery phrases. The Osmosis protocol does not define standards for private key storage; key management is handled at the wallet or client level, including software and hardware wallets compatible with the Cosmos SDK.

3. Modular Design and Smart Contracting

Osmosis follows a modular architecture based on the Cosmos SDK. Core protocol functionality, including the AMM and liquidity pool logic, is implemented at the application layer. Additional smart-contract functionality is provided through a permissioned CosmWasm module, whereby contract deployments require on-chain governance approval, ensuring that token logic and application-level rules added to the protocol remain subject to community oversight.

The following applies to Fantom:

Since the migration from the Fantom ecosystem to the Sonic ecosystem is ongoing, the Fantom Opera network should be understood as legacy infrastructure, while the Sonic network represents the successor network and the primary focus of ongoing ecosystem development. Fantom Opera continues to exist during a transitional period; however, Sonic Labs has announced that remaining legacy Opera infrastructure, including the Opera FTM-to-S bridge, is expected to be retired on 30

June 2026 at 17:00 GMT. Historical chain data is expected to remain preserved, while future technical development and operational focus are directed towards Sonic.

The following applies to Ethereum:

1. Decentralised Ledger: The Ethereum blockchain acts as a decentralised ledger for all ETH transactions, maintaining an append-only record of transfers and account balances to support transparency and verifiable settlement.
2. Account Model: Ethereum uses two account types: externally owned accounts (EOAs), which are controlled through private keys, and contract accounts, which are controlled through deployed smart contract code. Following the Pectra upgrade on 2025-05-07, EOAs can additionally authorise delegated code execution through EIP-7702 transactions without permanently converting the account into smart contracts.
3. Private Key Management: Users must securely store the private keys and recovery material associated with their wallets. Loss or compromise of a private key may result in irreversible loss of access to the associated ETH balance.
4. Cryptographic Integrity: Ethereum uses ECDSA over the secp256k1 elliptic curve for key generation and digital signatures on the execution layer. Keccak-256 hashing is used for transaction hashing, state hashing and address derivation. Ethereum addresses are derived from the last 20 bytes of the Keccak-256 hash of the public key. On the consensus layer, BLS (Boneh-Lynn-Shacham) signatures are used to aggregate validator attestations under the Proof-of-Stake consensus mechanism.

The following applies to Binance Smart Chain:

1. BSC-compatible wallets

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

2. Decentralised Ledger

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

3. BEP-20 token standard

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

4. Scalability and transaction efficiency

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

H.4 Consensus mechanism

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

The following applies to BandChain:

BandChain operates a Delegated Proof-of-Stake (DPoS) consensus mechanism based on Tendermint Byzantine Fault Tolerance, designed to provide deterministic finality and secure state replication.

Consensus participants are validators who bond the native crypto-asset BAND and obtain voting power proportional to their bonded stake, including stake delegated by token holders. Only a limited active validator set is permitted to participate in block production and consensus. Following Band v3 and BCIP-17, Band publicly described the Band Active Validators Set as comprising 53 validators, selected on the basis of operational reliability, technical performance, and ecosystem participation.

Consensus proceeds in rounds consisting of block proposal and voting phases. A block is considered final and irreversibly committed once more than two-thirds of total validator voting power signs the corresponding pre-commit vote. This mechanism provides immediate finality and prevents probabilistic forks.

The protocol remains secure provided that less than one-third of validator voting power behaves maliciously or fails. In addition to standard block validation, BandChain employs a validator sampling mechanism for oracle operations, whereby subsets of validators are randomly selected to fulfil data requests, reducing bottlenecks and enhancing decentralisation.

Delegators may assign their BAND tokens to validators without transferring custody, thereby participating indirectly in consensus and sharing in associated rewards and risks.

The following applies to Osmosis:

Osmosis operates a Proof-of-Stake consensus mechanism based on the Cosmos SDK and CometBFT, formerly Tendermint Core. CometBFT provides Byzantine Fault Tolerant state-machine replication for application-specific blockchains and is designed to provide deterministic finality once the required validator voting threshold is reached.

Consensus participants are validators who bond OSMO, or receive delegated OSMO from third-party token holders. Validator voting power is determined by the amount of OSMO bonded to the validator, including delegated stake. Validators participate in block production and consensus by proposing blocks and signing votes.

The active validator set is limited by protocol parameters. Current public parameter data indicates a maximum active validator set of 100 validators, following governance changes that reduced the set from 120 to 100 to improve performance and reduce consensus overhead.

Consensus proceeds through proposal and voting rounds. A block is committed once more than two-thirds of the total validator voting power has signed the relevant pre-commit for that block. This provides immediate finality and avoids probabilistic forks, provided that less than one-third of total validator voting power behaves maliciously or fails.

Osmosis also uses slashing and jailing mechanisms to support validator accountability. Current public parameter data indicates a 5% slash for double-signing, no direct slash for downtime, and a downtime jail duration of one minute. Validators that fail operational requirements may be removed from the active validator set until they rejoin in accordance with protocol rules. Delegators are exposed to validator-related slashing risk through the validators to whom they delegate.

The following applies to Fantom:

Since the migration from the Fantom ecosystem to the Sonic ecosystem is ongoing, the Fantom Opera network should be understood as legacy infrastructure, while the Sonic network represents the successor network and the primary focus of ongoing ecosystem development. Fantom Opera continues to exist during a transitional period; however, Sonic Labs has announced that remaining legacy Opera infrastructure, including the Opera FTM-to-S bridge, is expected to be retired on 30 June 2026 at 17:00 GMT. Historical chain data is expected to remain preserved, while future technical development and operational focus are directed towards Sonic.

The following applies to Ethereum:

Ethereum uses a Proof-of-Stake (PoS) consensus mechanism introduced with The Merge on 2022-09-15, which replaced the previous Proof-of-Work consensus model. The PoS mechanism is implemented through Gasper, combining Casper-FFG for finality with the LMD-GHOST fork-choice rule for chain selection. Validators participate in consensus by staking ETH through the Beacon Chain. Validators are pseudo-randomly selected to propose new blocks, while other validators attest to the validity of proposed blocks. The network operates using 12-second slots grouped into epochs of 32 slots. Under normal network conditions, finality is typically achieved after two epochs, approximately 12.8 minutes, through Casper-FFG. The LMD-GHOST fork-choice rule determines the canonical chain based on the accumulated weight of validator attestations. Validators that engage in certain malicious behaviour, such as equivocation or contradictory attestations, may be subject to slashing penalties, while offline validators may incur inactivity penalties. Subsequent network upgrades, including Dencun (2024-03-13), Pectra (2025-05-07) and Fusaka (2025-12-03), introduced protocol changes affecting Ethereum's consensus mechanism and Layer 2 functionality.

The following applies to Binance Smart Chain:

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

Core components

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

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

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

Consensus process

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

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

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

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

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

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

H.5 Incentive mechanisms and applicable fees

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

The following applies to BandChain:

The BandChain network employs an integrated system of economic incentives and penalties to secure its Delegated Proof-of-Stake consensus mechanism and to ensure reliable oracle data provision.

1. Incentive Mechanisms (Rewards)

Validators and delegators are rewarded for participating in block production and oracle operations through a combination of inflationary issuance and transaction-related fees. New BAND tokens are issued as block rewards under a dynamic inflation model. The inflation rate adjusts within a predefined range to incentivise staking participation and is designed to target a specific proportion of total supply being bonded. Rewards are distributed to validators and their delegators in proportion to their bonded stake, subject to validator-defined commission rates. Additional rewards may be allocated to participants involved in specialised roles, such as Threshold Signature Scheme operations.

2. Transaction Fees

The protocol applies transaction fees to all on-chain operations to prevent network abuse and compensate validators. Fees are determined based on transaction complexity and are paid by the initiating party. In the context of oracle operations, additional fees may be required for accessing premium data sources. For cross-chain requests, fees may be paid by relayer accounts acting on behalf of external users.

3. Fee Distribution and Community Pool

Collected transaction fees and newly issued tokens are distributed to validators and delegators. A predefined portion of block rewards is allocated to a community fund pool, which is intended to support long-term ecosystem development and is governed through on-chain governance decisions. In addition, certain fees related to oracle data requests may be allocated directly to data providers or associated service accounts.

4. Penalties and Slashing

Bonded BAND tokens serve as economic collateral and are subject to slashing in the event of protocol violations. Validators that engage in safety violations, such as double-signing conflicting blocks, are subject to significant slashing and removal from the validator set. Validators may also be penalised for excessive downtime or failure to fulfil assigned oracle data requests. Jailing mechanisms may temporarily exclude validators from participation until operational requirements

are restored. Delegators are exposed to slashing risks through the validators to whom they delegate.

The following applies to Osmosis:

1. Validator and Delegator Rewards

Validators earn rewards from transaction fees and protocol emissions for their role in securing the network and processing transactions. Rewards are distributed in OSMO tokens. Delegators who stake their OSMO tokens with validators receive a proportional share of these rewards. New OSMO tokens are issued on an epoch basis (approximately once per day) and allocated in part to staking rewards. The allocation of newly issued tokens is subject to protocol governance and may be adjusted over time.

2. Liquidity Provider Incentives

Users providing liquidity to Osmosis pools earn swap fees generated by trading activity and may receive additional incentives in the form of OSMO tokens. These incentives are designed to support liquidity depth and trading efficiency on the protocol. The level and structure of such incentives may be adjusted through governance.

3. Transaction Fees

Users pay transaction fees in OSMO tokens, or in certain whitelisted assets, for network activities including swaps, staking, and governance participation. These fees are distributed to validators and delegators, contributing to their ongoing economic incentives.

4. Slashing and Penalties

To discourage malicious or negligent behaviour, the protocol employs a bonded proof-of-stake model in which validators' staked assets may be subject to slashing. Validators that engage in protocol violations, such as double-signing, may incur a reduction of their staked assets. Validators that fail to meet operational requirements, such as maintaining sufficient uptime, may be temporarily removed from the active validator set. Delegators are exposed to the risks associated with the validators to whom they delegate.

The following applies to Fantom:

Since the migration from the Fantom ecosystem to the Sonic ecosystem is ongoing, the Fantom Opera network should be understood as legacy infrastructure, while the Sonic network represents the successor network and the primary focus of ongoing ecosystem development. Fantom Opera continues to exist during a transitional period; however, Sonic Labs has announced that remaining legacy Opera infrastructure, including the Opera FTM-to-S bridge, is expected to be retired on 30 June 2026 at 17:00 GMT. Historical chain data is expected to remain preserved, while future technical development and operational focus are directed towards Sonic.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

Incentive mechanisms

1. Validators: Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure.
2. Delegators: BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission.
3. Candidates: BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information.
4. Economic Security: Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance.

Fees on the Binance Smart Chain

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

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

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

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

H.6 Use of distributed ledger technology

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

H.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

Regulatory frameworks applicable to crypto-asset services in the European Union and in third countries are evolving. Supervisory authorities may introduce, interpret, or enforce rules that affect (i) the eligibility of this crypto-asset for admission to trading, (ii) the conditions under which a crypto-asset service provider may offer trading, custody, or transfer services for it, or (iii) the persons or jurisdictions to which such services may be provided. As a result, the crypto-asset service provider

admitting this crypto-asset to trading may be required to suspend, restrict, or terminate trading or withdrawals for regulatory reasons, even if the crypto-asset itself continues to function on its underlying network.

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

Delays, failures, or changes in the implementation of the project as outlined in its public roadmap or technical documentation may negatively impact the perceived credibility or usability of the crypto-

asset. This includes risks related to project governance, resource allocation, technical delivery, and team continuity.

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG001FE242

S.3 Name of the crypto-asset

Band

S.4 Consensus Mechanism

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

The following applies to BandChain:

BandChain operates a Delegated Proof-of-Stake (DPoS) consensus mechanism based on Tendermint Byzantine Fault Tolerance, designed to provide deterministic finality and secure state replication.

Consensus participants are validators who bond the native crypto-asset BAND and obtain voting power proportional to their bonded stake, including stake delegated by token holders. Only a limited active validator set is permitted to participate in block production and consensus. Following Band v3 and BCIP-17, Band publicly described the Band Active Validators Set as comprising 53 validators, selected on the basis of operational reliability, technical performance, and ecosystem participation.

Consensus proceeds in rounds consisting of block proposal and voting phases. A block is considered final and irreversibly committed once more than two-thirds of total validator voting power signs the corresponding pre-commit vote. This mechanism provides immediate finality and prevents probabilistic forks.

The protocol remains secure provided that less than one-third of validator voting power behaves maliciously or fails. In addition to standard block validation, BandChain employs a validator sampling mechanism for oracle operations, whereby subsets of validators are randomly selected to fulfil data requests, reducing bottlenecks and enhancing decentralisation.

Delegators may assign their BAND tokens to validators without transferring custody, thereby participating indirectly in consensus and sharing in associated rewards and risks.

The following applies to Osmosis:

Osmosis operates a Proof-of-Stake consensus mechanism based on the Cosmos SDK and CometBFT, formerly Tendermint Core. CometBFT provides Byzantine Fault Tolerant state-machine replication for application-specific blockchains and is designed to provide deterministic finality once the required validator voting threshold is reached.

Consensus participants are validators who bond OSMO, or receive delegated OSMO from third-party token holders. Validator voting power is determined by the amount of OSMO bonded to the validator, including delegated stake. Validators participate in block production and consensus by proposing blocks and signing votes.

The active validator set is limited by protocol parameters. Current public parameter data indicates a maximum active validator set of 100 validators, following governance changes that reduced the set from 120 to 100 to improve performance and reduce consensus overhead.

Consensus proceeds through proposal and voting rounds. A block is committed once more than two-thirds of the total validator voting power has signed the relevant pre-commit for that block. This provides immediate finality and avoids probabilistic forks, provided that less than one-third of total validator voting power behaves maliciously or fails.

Osmosis also uses slashing and jailing mechanisms to support validator accountability. Current public parameter data indicates a 5% slash for double-signing, no direct slash for downtime, and a downtime jail duration of one minute. Validators that fail operational requirements may be removed from the active validator set until they rejoin in accordance with protocol rules. Delegators are exposed to validator-related slashing risk through the validators to whom they delegate.

The following applies to Fantom:

Since the migration from the Fantom ecosystem to the Sonic ecosystem is ongoing, the Fantom Opera network should be understood as legacy infrastructure, while the Sonic network represents the successor network and the primary focus of ongoing ecosystem development. Fantom Opera continues to exist during a transitional period; however, Sonic Labs has announced that remaining legacy Opera infrastructure, including the Opera FTM-to-S bridge, is expected to be retired on 30 June 2026 at 17:00 GMT. Historical chain data is expected to remain preserved, while future technical development and operational focus are directed towards Sonic.

The following applies to Ethereum:

Ethereum uses a Proof-of-Stake (PoS) consensus mechanism introduced with The Merge on 2022-09-15, which replaced the previous Proof-of-Work consensus model. The PoS mechanism is implemented through Gasper, combining Casper-FFG for finality with the LMD-GHOST fork-choice rule for chain selection. Validators participate in consensus by staking ETH through the Beacon Chain. Validators are pseudo-randomly selected to propose new blocks, while other validators attest to the validity of proposed blocks. The network operates using 12-second slots grouped into epochs of 32 slots. Under normal network conditions, finality is typically achieved after two epochs, approximately 12.8 minutes, through Casper-FFG. The LMD-GHOST fork-choice rule determines the canonical chain based on the accumulated weight of validator attestations. Validators that engage in certain malicious behaviour, such as equivocation or contradictory attestations, may be subject to slashing penalties, while offline validators may incur inactivity penalties. Subsequent network upgrades, including Dencun (2024-03-13), Pectra (2025-05-07) and Fusaka (2025-12-03), introduced protocol changes affecting Ethereum's consensus mechanism and Layer 2 functionality.

The following applies to Binance Smart Chain:

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

Core components

1. Validators (Cabinet and Candidates): Validators are responsible for producing blocks, validating transactions, and maintaining network security. The validator set consists of up to 45 validators, including 21 "Cabinet" validators and 24 "Candidate" validators, selected based on bonded stake. A subset of validators is selected per epoch to participate in block production.
2. Delegators: Token holders may delegate BNB to validators to support their selection. Delegators share in the rewards generated by validators, providing an economic incentive to participate in staking.
3. Candidates: Validator candidates are nodes that have staked BNB but are not part of the primary validator subset for a given epoch. They may be selected into the active set based on staking rank and can participate in block production with lower probability.

Consensus process

4. Validator selection: Validators are ranked based on the amount of bonded BNB and are updated periodically (approximately every 24 hours). The highest-ranked validators form the active validator set, with Cabinet validators having a higher probability of participating in block production.
5. Block production: Validators take turns producing blocks in a PoA-like manner. For each epoch, a subset of validators is selected to produce and validate blocks sequentially, ensuring high throughput and low latency.
6. Transaction finality: BSC achieves short block times (approximately 0.45 seconds) and fast finality. With Fast Finality enabled, blocks are typically finalised within approximately one second, subject to validator participation.
7. Staking: Validators must stake BNB as collateral and may be subject to slashing in cases of misbehaviour, including double-signing, malicious voting, or prolonged downtime.
8. Delegation and rewards: Validators and delegators are rewarded through transaction fees collected in each block. Validators may share rewards with delegators to attract stake.
9. Transaction fees: BSC does not rely on inflationary block rewards; instead, validators are compensated primarily through transaction fees paid in BNB, aligning incentives with network usage.

S.5 Incentive Mechanisms and Applicable Fees

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

The following applies to BandChain:

The BandChain network employs an integrated system of economic incentives and penalties to secure its Delegated Proof-of-Stake consensus mechanism and to ensure reliable oracle data provision.

1. Incentive Mechanisms (Rewards)

Validators and delegators are rewarded for participating in block production and oracle operations through a combination of inflationary issuance and transaction-related fees. New BAND tokens are issued as block rewards under a dynamic inflation model. The inflation rate adjusts within a predefined range to incentivise staking participation and is designed to target a specific proportion of total supply being bonded. Rewards are distributed to validators and their delegators in proportion to their bonded stake, subject to validator-defined commission rates. Additional rewards

may be allocated to participants involved in specialised roles, such as Threshold Signature Scheme operations.

2. Transaction Fees

The protocol applies transaction fees to all on-chain operations to prevent network abuse and compensate validators. Fees are determined based on transaction complexity and are paid by the initiating party. In the context of oracle operations, additional fees may be required for accessing premium data sources. For cross-chain requests, fees may be paid by relayer accounts acting on behalf of external users.

3. Fee Distribution and Community Pool

Collected transaction fees and newly issued tokens are distributed to validators and delegators. A predefined portion of block rewards is allocated to a community fund pool, which is intended to support long-term ecosystem development and is governed through on-chain governance decisions. In addition, certain fees related to oracle data requests may be allocated directly to data providers or associated service accounts.

4. Penalties and Slashing

Bonded BAND tokens serve as economic collateral and are subject to slashing in the event of protocol violations. Validators that engage in safety violations, such as double-signing conflicting blocks, are subject to significant slashing and removal from the validator set. Validators may also be penalised for excessive downtime or failure to fulfil assigned oracle data requests. Jailing mechanisms may temporarily exclude validators from participation until operational requirements are restored. Delegators are exposed to slashing risks through the validators to whom they delegate.

The following applies to Osmosis:

1. Validator and Delegator Rewards

Validators earn rewards from transaction fees and protocol emissions for their role in securing the network and processing transactions. Rewards are distributed in OSMO tokens. Delegators who stake their OSMO tokens with validators receive a proportional share of these rewards. New OSMO tokens are issued on an epoch basis (approximately once per day) and allocated in part to staking rewards. The allocation of newly issued tokens is subject to protocol governance and may be adjusted over time.

2. Liquidity Provider Incentives

Users providing liquidity to Osmosis pools earn swap fees generated by trading activity and may receive additional incentives in the form of OSMO tokens. These incentives are designed to support liquidity depth and trading efficiency on the protocol. The level and structure of such incentives may be adjusted through governance.

3. Transaction Fees

Users pay transaction fees in OSMO tokens, or in certain whitelisted assets, for network activities including swaps, staking, and governance participation. These fees are distributed to validators and delegators, contributing to their ongoing economic incentives.

4. Slashing and Penalties

To discourage malicious or negligent behaviour, the protocol employs a bonded proof-of-stake model in which validators' staked assets may be subject to slashing. Validators that engage in protocol violations, such as double-signing, may incur a reduction of their staked assets. Validators that fail to meet operational requirements, such as maintaining sufficient uptime, may be temporarily removed from the active validator set. Delegators are exposed to the risks associated with the validators to whom they delegate.

The following applies to Fantom:

Since the migration from the Fantom ecosystem to the Sonic ecosystem is ongoing, the Fantom Opera network should be understood as legacy infrastructure, while the Sonic network represents the successor network and the primary focus of ongoing ecosystem development. Fantom Opera continues to exist during a transitional period; however, Sonic Labs has announced that remaining legacy Opera infrastructure, including the Opera FTM-to-S bridge, is expected to be retired on 30 June 2026 at 17:00 GMT. Historical chain data is expected to remain preserved, while future technical development and operational focus are directed towards Sonic.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

Incentive mechanisms

1. **Validators:** Validators must self-delegate BNB in order to participate in the validator system. Validator selection is staking-based, and validators that rank highly enough enter the active set and participate in block production and transaction validation. Validators are rewarded from transaction fees collected on the network. When a block is produced, most of the block fee is allocated to the validator that proposed the block. A portion is retained as validator commission, while the remainder is allocated for distribution through the validator credit structure.
2. **Delegators:** BNB holders may delegate BNB to validators. This increases the validator's total stake and may improve its position in the validator ranking. Delegators share in the rewards earned by the validator they support, after deduction of the validator's commission.
3. **Candidates:** BSC distinguishes between Cabinet, Candidate and Inactive validators. The current model provides that the top 21 validators form the Cabinet, while the validators ranked from 22 to 45 are Candidates. Candidate validators have a smaller chance of producing blocks, but they remain part of the broader validator structure and support network resilience. Validator roles are updated every 24 hours based on the latest staking information.
4. **Economic Security:** Validators may be penalised for misconduct or poor performance. Slashable events include double signing, malicious fast-finality voting and unavailability. Depending on the violation, consequences may include removal from the validator set, loss of staking rewards and slashing of part of the validator's self-delegated BNB. The staking model therefore creates an economic incentive for validators and delegators to support reliable validator performance.

Fees on the Binance Smart Chain

5. **Transaction fees:** Transaction fees on BSC are paid in BNB and are intended to compensate validators for maintaining the network. BSC is designed as a comparatively low-fee network, and smart-contract transactions and transfers require gas fees in BNB.
6. **Validator rewards:** BSC does not rely on a separate protocol-level block reward. Instead, staking rewards are derived from transaction fees. Most of the block fee is allocated to the proposing validator, then split between validator commission and delegator-linked reward distribution.
7. **System-level fee allocation:** Part of transaction-fee revenue is collected through the System Reward Contract and used for designated system purposes, including fast-finality rewards.
8. **Smart contract fees:** Deploying and interacting with smart contracts on BSC requires payment of gas fees in BNB. These fees depend on the computational resources required and form part of the network's overall fee and validator-incentive model.

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

2025-05-17

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

2026-05-17

S.8 Energy consumption

28821.99728 kWh/a

S.9 Energy consumption sources and methodologies

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

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

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

S.10 Renewable energy consumption

34.1398258401 %

S.11 Energy intensity

0.00012 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO₂e/a

S.13 Scope 2 DLT GHG emissions – Purchased

9.59234 tCO₂e/a

S.14 GHG intensity

0.00004 kgCO₂e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivisation structure and consensus mechanism.

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

S.16 Key GHG sources and methodologies

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

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

