

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

Preamble

00. Table of Content

Preamble	2
01. Date of notification	8
02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	8
03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	8
04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114	8
05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114	8
06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114	8
Summary	8
07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114	8
08. Characteristics of the crypto-asset	8
09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	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	11
A.7 Another identifier required pursuant to applicable national law	11
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	13

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	14
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	15
C.11 Operator business activity	15
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	16
D.8 Plans for the token	17
D.9 Resource allocation	18
D.10 Planned use of Collected funds or crypto-Assets	18
Part E – Information about the offer to the public of crypto-assets or their admission to trading	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	19
E.7 Oversubscription allocation	19
E.8 Issue price	19
E.9 Official currency or any other crypto-assets determining the issue price	19
E.10 Subscription fee	20
E.11 Offer price determination method	20
E.12 Total number of offered/traded crypto-assets	20
E.13 Targeted holders	20
E.14 Holder restrictions	20
E.15 Reimbursement notice	20
E.16 Refund mechanism	20
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	21
E.25 Value transfer methods for reimbursement	21
E.26 Right of withdrawal	21
E.27 Transfer of purchased crypto-assets	21

E.28 Transfer time schedule	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	22
E.37 Offer expenses	22
E.38 Conflicts of interest	22
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	23
F.3 Planned application of functionalities	24
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	25
F.8 Website of the issuer	25
F.9 Starting date of offer to the public or admission to trading	25
F.10 Publication date	25
F.11 Any other services provided by the issuer	25
F.12 Language or languages of the crypto-asset white paper	25
F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates	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	26
G.1 Purchaser rights and obligations	26
G.2 Exercise of rights and obligations	26
G.3 Conditions for modifications of rights and obligations	27
G.4 Future public offers	27
G.5 Issuer retained crypto-assets	27
G.6 Utility token classification	27
G.7 Key features of goods/services of utility tokens	27
G.8 Utility tokens redemption	27
G.9 Non-trading request	27
G.10 Crypto-assets purchase or sale modalities	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	28
G.15 Token value protection schemes description	28
G.16 Compensation schemes	28
G.17 Compensation schemes description	28
G.18 Applicable law	28
G.19 Competent court	28
Part H – information on the underlying technology	29
H.1 Distributed ledger technology (DTL)	29
H.2 Protocols and technical standards	29
H.3 Technology used	31
H.4 Consensus mechanism	33
H.5 Incentive mechanisms and applicable fees	36
H.6 Use of distributed ledger technology	38
H.7 DLT functionality description	38
H.8 Audit	39
H.9 Audit outcome	39
Part I – Information on risks	39
I.1 Offer-related risks	39
I.2 Issuer-related risks	41
I.3 Crypto-assets-related risks	41
I.4 Project implementation-related risks	44
I.5 Technology-related risks	44

I.6 Mitigation measures	46
Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts	47
J.1 Adverse impacts on climate and other environment-related adverse impacts	47
S.1 Name	47
S.2 Relevant legal entity identifier	47
S.3 Name of the cryptoasset	47
S.4 Consensus Mechanism	47
S.5 Incentive Mechanisms and Applicable Fees	49
S.6 Beginning of the period to which the disclosure relates	52
S.7 End of the period to which the disclosure relates	52
S.8 Energy consumption	52
S.9 Energy consumption sources and methodologies	52
S.10 Renewable energy consumption	53
S.11 Energy intensity	53
S.12 Scope 1 DLT GHG emissions – Controlled	53
S.13 Scope 2 DLT GHG emissions – Purchased	53
S.14 GHG intensity	53
S.15 Key energy sources and methodologies	53
S.16 Key GHG sources and methodologies	53

01. Date of notification

This white paper was notified on 2026-02-26.

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 Kyber Network Crystal (KNC) referred to in this white paper is a crypto-asset other than EMTs and ARTs and is issued on multiple blockchain networks, namely Ethereum, Binance Smart Chain, Polygon, Optimism, Arbitrum, as of 2026-02-23 and according to DTI FFG shown in F. 14. The maximum supply of the crypto-asset is currently fixed at 252,301,550 tokens. However due to KIP-6 in 2021, KNC was upgraded to a dynamic token supply. This allows the KyberDAO to mint or burn tokens as necessary to fund new protocol developments. The first activity on Ethereum can be viewed on 2021-04-12 (transaction hash: 0xf1558fa2757fc509172aab73bfbc6231f24005dcd5fe9105fef05b91620ffd, source: <https://etherscan.io/tx/0xf1558fa2757fc509172aab73bfbc6231f24005dcd5fe9105fef05b91620ffd>, accessed 2026-02-23). The first activity on Binance Smart Chain can be viewed on 2021-08-23 (transaction hash: 0x879bb2f5a0a80a5e9977c529c7abbe8bf5a32f293e3c815f8d066477563b473b, source: <https://bscscan.com/tx/0x879bb2f5a0a80a5e9977c529c7abbe8bf5a32f293e3c815f8d066477563b473b>, accessed 2026-02-23). The first activity on Polygon can be viewed on 2021-06-07 (transaction hash: 0xd43da05e12d53bfcd3f31edda2cf82943c3e423ea55ed25a5ad044b5d02de2ae, source: <https://polygonscan.com/tx/0xd43da05e12d53bfcd3f31edda2cf82943c3e423ea55ed25a5ad044b5d02de2ae>, accessed 2026-02-23). The first activity on Optimism can be viewed on 2022-08-18 (transaction hash: 0x8bca230959ea1f22394ae1d3a9109fc7df4a57cfbee8172aab366f8cc36e8616, source: <https://optimistic.etherscan.io/tx/0x8bca230959ea1f22394ae1d3a9109fc7df4a57cfbee8172aab366f8cc36e8616>, accessed 2026-02-23). The first activity on Arbitrum can be viewed on 2022-08-11 (transaction hash: 0x22d0f420e518d2bc104f31d8f526ff137467e776d7d28c8ecd73552d080cfd7, source: <https://arbiscan.io/tx/0x22d0f420e518d2bc104f31d8f526ff137467e776d7d28c8ecd73552d080cfd7>, accessed 2026-02-23).

The Kyber Network project is a decentralised finance initiative focused on providing liquidity infrastructure for digital asset markets. It operates as a multi-chain ecosystem centred around KyberSwap, a decentralised exchange platform that aggregates liquidity across multiple blockchain networks. The protocol is designed to connect traders to various on-chain liquidity sources through automated smart contracts, enabling token swaps, liquidity provision, and related decentralised finance functionalities without reliance on centralised intermediaries. KyberSwap incorporates liquidity aggregation mechanisms, specialised liquidity protocols, and developer-facing integration tools that allow third-party applications to access routing, swapping, and liquidity services. The system supports functionalities such as trade routing optimisation, limit order execution, liquidity pool participation, and cross-chain interactions, subject to network conditions and smart contract configurations.

Within this ecosystem, the KNC crypto-asset functions as a technical governance and incentive mechanism. KNC holders may stake their tokens in the KyberDAO to participate in on-chain governance processes, including voting on Kyber Improvement Proposals that relate to protocol parameters, fee configurations, and potential upgrades. Staked KNC may entitle participants, through smart contract logic, to receive a portion of protocol-generated trading fees, typically distributed in KNC or other designated assets. The token is also used within incentive frameworks, including liquidity mining programmes designed to encourage liquidity provision across supported pools. Following the implementation of KIP-6, KNC operates under a dynamic supply model in which token minting or burning may occur based on governance decisions of the KyberDAO, including for the purpose of protocol development or ecosystem incentives. These mechanisms are implemented through smart contracts and are subject to governance outcomes and technical constraints.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

Crypto Risk Metrics GmbH, founded in 2018 and based in Hamburg (HRB 154488), has undergone several strategic shifts in its business focus since incorporation. Due to these changes in business model and operational direction over time, the financial figures from earlier years are only comparable to a limited extent with the company's current commercial activities. The present

business model – centred on regulatory technology and risk analytics in the context of the MiCA framework – has been developed progressively and can realistically be considered fully operational since approximately 2024.

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

KYBER NETWORK PTE. LTD.

B.3 Legal form

The legal form of KYBER NETWORK PTE. LTD. is IWZF, which corresponds to "Private Company Limited by Shares".

B.4 Registered address

The registered address of KYBER NETWORK PTE. LTD. is 1 Upper Circular Road, #05-01, 058400,

Singapore

SG-01

B.5 Head office

Could not be identified.

Could not be identified.

Could not be identified.

B.6 Registration date

KYBER NETWORK PTE. LTD. was registered on 2017-07-13.

B.7 Legal entity identifier

KYBER NETWORK PTE. LTD. has no Legal Entity Identifier (LEI).

B.8 Another identifier required pursuant to applicable national law

Unique Entity Number (UEN): 201719741W

B.9 Parent company

No parent company of KYBER NETWORK PTE. LTD. can be identified.

B.10 Members of the management body

Identity	Function	Business Address
Luu The Loi	Co-founder of Kyber	Cannot be identified.

B.11 Business activity

This Company's principal activity is development of software and applications (except games and cybersecurity) with other financial service activities, except insurance and pension funding activities n.e.c. as the secondary activity.

B.12 Parent company business activity

Not applicable.

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

C.1 Name

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

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-Asset white paper Preparation

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

C.10 Members of the Management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

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

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

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

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

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

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Kyber Network Crystal v2", Short Name: "KNC" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-23).

D.2 Crypto-assets name

Long Name: "Kyber Network Crystal v2" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-23).

D.3 Abbreviation

Short Name: "KNC" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-23).

D.4 Crypto-asset project description

According to public information (source: <https://docs.kyberswap.com/>, accessed 2026-02-23), the Kyber Network project is a crypto-asset initiative concerned with the development and operation of an open and permissionless liquidity infrastructure designed to support decentralised trading and capital efficiency across multiple distributed-ledger networks. The project centres on KyberSwap, a multi-chain decentralised exchange aggregator and liquidity platform that connects users to numerous liquidity sources across various blockchain networks. The protocol architecture includes aggregation mechanisms for routing trades across decentralised exchanges, liquidity-management modules for yield optimisation, and developer-facing tools such as APIs and integration widgets intended to enable third-party applications to access Kyber's trading infrastructure. The project is maintained by contributors to the Kyber Network ecosystem and is intended to provide users and developers with tools for interacting with decentralised financial systems in a multi-chain environment, subject to the availability, performance, and continued operation of the underlying technological infrastructure.

The KNC crypto-asset functions as an element within this broader technical framework. It is intended to interact with specific parts of the protocol's internal logic, such as governance parameters, staking modules, fee-distribution mechanisms, and liquidity-incentive structures, if and when these features are implemented or activated. KNC may be staked within the KyberDAO governance system to participate in voting on protocol-related proposals, including changes to fee configurations, upgrades, or ecosystem initiatives. Certain functionalities, such as governance reward distributions, liquidity mining incentives, gas-related benefits, or supply-adjustment mechanisms, remain contingent on technical implementation, governance decisions, and operational priorities. There is no assurance that any proposed or potential functionalities will be introduced, remain active, or be accessible at all times.

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 KNC crypto-asset may serve as a governance and utility input for certain protocol processes. The long-term evolution of the Kyber Network system, including the scope of available features, the governance roadmap, validator or liquidity-participant selection mechanisms, and the operational continuity of the infrastructure, may vary based on technical, economic, and regulatory considerations. All future developments remain subject to change.

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
Victor Tran	Other person involved in implementation	Cannot be found	Cannot be found
Loi Luu	Other person involved in implementation	Cannot be found	Cannot be found
Kyber Network Pte. Ltd.	Other person involved in implementation	1 Upper Circular Road, #05-01, Singapore (058400)	Singapore

D.6 Utility Token Classification

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

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

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”.

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

D.8 Plans for the token

This section provides an overview of the historical developments related to the KNC 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 KNC crypto-asset and/or the Kyber Network protocol. Based on the official roadmap (sources: <https://docs.kyberswap.com/>, <https://blog.kyberswap.com/>, <https://blog.kyberswap.com/kyberswap-product-roadmap-updates-2025/>; accessed 2026-02-23), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Kyber Network protocol and the role of the KNC crypto-asset.

Past milestones:

- Initial Coin Offering (16 September 2017): The token generation event concluded, raising 200,000 ETH and minting 226,000,000 KNC tokens, thereby establishing the initial supply and distribution framework of the crypto-asset.
- Kyber 3.0 Upgrade Announcement (21 January 2021): The transition to “Kyber 3.0” was announced, restructuring the network from a single protocol into a hub of liquidity protocols, thereby affecting the technical architecture and the economic role of KNC within governance and protocol coordination.
- KNC Token Migration (20 April 2021): Following approval under KIP-6, the migration from the legacy KNC token (renamed KNCL) to a new KNC token commenced at a 1:1 ratio, introducing updated token mechanics intended to enhance flexibility in governance and fee-related parameters.
- Minting for Ecosystem Growth Fund (15 June 2021): KyberDAO approved the minting of 42,050,588 additional KNC under KIP-8 and KIP-9 to fund ecosystem growth initiatives, resulting in an increase in total token supply.
- KyberSwap Elastic Security Incident (22 November 2023): A security incident affected the KyberSwap Elastic protocol, leading to the subsequent discontinuation of the Elastic and Classic liquidity services and materially impacting certain protocol components.
- FairFlow Launch and Trading Volume Milestone (August 2025): Reported launch of FairFlow, a liquidity mechanism intended to capture arbitrage value for liquidity providers.

Future milestones:

- Biannual Roadmap Updates (2026): The project has communicated its intention to review and publish updated roadmaps twice per year to inform stakeholders of progress and adjustments to planned developments.

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

D.9 Resource allocation

Based on information from various third-party and industry sources, it is reported that Kyber Network's primary capital-raising event related to the KNC crypto-asset was an Initial Coin Offering (ICO) completed in 2017. The sources provided do not describe a documented sequence of traditional venture capital financing rounds (for example, Series A or Series B) directly attributable to the KNC token, and any references to external support mechanisms or institutional involvement are limited and not verifiable via regulatory filings or issuer confirmations. As a result, the information below should be considered indicative only and cannot be independently verified.

Based on the provided sources, Kyber Network is reported to have concluded its KNC token sale on or around 2017-09-16, raising approximately 200,000 ETH on Ethereum. This event is described as having involved a large number of participating addresses and is referenced as the main historical fundraising event associated with KNC. Based on publicly available third-party sources, 19.47% of the initial KNC token supply, corresponding to 44,002,200 KNC, was reportedly allocated to company operational reserves as part of the 2017 ICO distribution.

Reported Institutional Links and External Support (Non-Exhaustive)

- External grants and incentives: It is reported that the Uniswap Foundation provided incentives exceeding USD 100,000 in 2025 to support adoption of Kyber-related FairFlow hooks.

- KyberDAO Ecosystem Growth Fund minting: It is reported that KyberDAO governance approved the minting of additional KNC in 2021 (referenced as 42,050,588 KNC) for an ecosystem growth fund intended to support liquidity and adoption. This reflects a governance decision on token supply and allocation, not a third-party capital raise, and the downstream use of these resources cannot be verified from the provided information.

Overall, the only consistently referenced fundraising event in the provided materials is the 2017 ICO. Any broader conclusions about venture capital financing, investor identities, or the current availability and allocation of historical proceeds would require issuer-confirmed disclosures or verifiable primary documentation, which are not available based on the information provided.

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

While historical sources and governance documentation refer to an aggregate token supply of 252,301,550 KNC, reflecting legacy token states and migration mechanics, the currently active Kyber Network Crystal v2 (KNC) token contract on Ethereum reflects a total supply of 240,896,837 KNC as of 2026-02-23 (source: <https://etherscan.io/token/0xdeFA4e8a7bcBA345F687a2f1456F5Edd9CE97202>).

The higher figure represents cumulative historical supply accounting across legacy and migrated token representations. The lower figure corresponds to the amount presently instantiated under the active ERC-20 token contract, which is primarily referenced for trading and liquidity purposes. Accordingly, not all historically referenced token units are necessarily reflected in the currently active contract state.

Following the approval of KIP-6 in 2021, KNC operates under a DAO-controlled dynamic supply model. Under this framework, the KyberDAO may, subject to governance procedures and participation thresholds, authorise minting or burning of KNC. The token is therefore not strictly hard capped. Both historically reported aggregate supply figures and the currently instantiated on-chain supply may change over time as governance decisions are implemented and reflected on the relevant blockchain networks.

Changes in effective supply, including governance-authorized minting or burning events, may affect token scarcity, circulating supply metrics, liquidity conditions, and market value. The circulating supply may therefore differ from historical aggregate supply figures as well as from the total supply reflected under the active token contract 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 to any additional restrictions such provider may impose.

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

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

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

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

F.2 Crypto-asset functionality

According to public information available on the official website (<https://docs.kyberswap.com/>, accessed 2026-02-23) and associated governance and documentation resources, the KNC token is an Ethereum ERC-20 token intended to operate as the primary on-chain coordination mechanism within the Kyber Network ecosystem. KNC was originally deployed on the Ethereum blockchain and

is designed to interact with smart-contract based infrastructure supporting trading aggregation, liquidity provision, and protocol governance. In addition to its Ethereum deployment, representations or bridged versions of KNC may be available on other blockchain networks in connection with Kyber's multi-chain expansion, subject to the technical configuration and bridge mechanisms used.

The KNC token is designed to facilitate decentralized decision-making within the Kyber protocol environment. Token holders may stake KNC in the KyberDAO and participate in governance processes, including proposing and voting on Kyber Improvement Proposals that determine protocol-level parameters such as fee structures, incentive mechanisms, treasury allocations, and technical upgrades. Voting rights relate exclusively to technical and protocol-level features and do not extend to decisions regarding the operation, management, or assets of any legal entity associated with the project.

Within the Kyber ecosystem, KNC may be used in connection with staking mechanisms that enable participation in governance and eligibility for protocol-defined incentive distributions funded by a portion of trading fees. The token may also be used in liquidity mining programs and other incentive schemes intended to promote liquidity provision and ecosystem participation. These functionalities depend on the stable operation of the underlying smart contracts, the security of validator and bridge infrastructure where applicable, the correct execution of governance-approved parameters, and the continued availability and performance of the relevant blockchain networks.

The KNC 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 Kyber protocol environment. The actual usability of KNC depends on factors such as system stability, smart-contract execution, development progress, governance decisions, and the operational conditions of the Ethereum blockchain, which are outside the control of token holders.

F.3 Planned application of functionalities

Future milestones:

- Biannual Roadmap Updates (2026): The project has communicated its intention to review and publish updated roadmaps twice per year to inform stakeholders of progress and adjustments to planned developments.

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

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

F.7 Commercial name or trading name

Long Name: "Kyber Network Crystal v2" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-02-23).

F.8 Website of the issuer

<https://kyber.network/>

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

2026-03-30

F.10 Publication date

2026-03-30

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

8JTDJ95PK, HJ1K3JQ1C, ZLX3SSPX5, HFT3N3C48, 291SG90B8

F.14 Functionally fungible group digital token identifier

L0DZSBLVZ

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

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

Accordingly, holders do not acquire any 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 were not available at the time of writing this white paper (2026-02-23).

G.5 Issuer retained crypto-assets

According to publicly available information on the official website (<https://docs.kyberswap.com/governance/knc-token/knc-tokenomics>, accessed on 2026-02-23), KYBER NETWORK PTE. LTD. was allocated 19.47% of the initial KNC token supply, corresponding to 44,002,200 KNC, as part of the 2017 ICO distribution. This allocation was reportedly designated for the Company's operational reserves. These crypto-assets therefore form part of the Company's treasury holdings.

Note: Although the allocation to KYBER NETWORK PTE. LTD. is publicly disclosed, the on-chain wallet addresses associated with this allocation cannot be independently linked to specific natural persons. Token transfers, treasury management activities, or other internal reallocations may occur without prior notice and could affect the concentration of holdings and any governance influence associated with these assets. The current token distribution can be traced on-chain at: <https://etherscan.io/token/0xdeFA4e8a7bcBA345F687a2f1456F5Edd9CE97202#balances>.

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 2026-02-23.

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 by Crypto Risk Metrics GmbH, which is established in Germany. Accordingly, this white paper shall be governed by the laws of the Federal Republic of Germany.

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

The crypto-asset in scope is implemented on the Ethereum Ether, Binance Smart Chain, Polygon POL, Optimism and Arbitrum networks following the standards described below.

H.2 Protocols and technical standards

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

The following applies to Ethereum Ether:

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

1. Network Protocols

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

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

2. Transaction and Address Standards

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

Transaction Types:

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

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

3. Blockchain Data Structure & Block Standards

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

Each block contains:

- Block Header: Parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, proposer signature.

- Transactions: Smart contract executions and token transfers.

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

4. Upgrade & Improvement Standards

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

The following applies to Binance Smart Chain:

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

The following applies to Polygon POL:

The Polygon network is built on a clear set of protocols and standards designed to ensure scalability, interoperability, and security. Polygon is built on top of Ethereum, it combines Layer-2 features with sidechain architecture. Network security is provided through Proof-of-Stake, where validators stake POL to propose and validate blocks. The consensus architecture consists of three layers: Smart Contracts on Ethereum that are used for staking POL. The Heimdall layer consisting of Heimdall nodes running in parallel to the Ethereum mainnet, monitoring the staking smart contracts deployed on the mainnet, and committing checkpoints to the mainnet. And the Bor layer, which are block producing Bor nodes. Bor clients are based on the widely used Go Ethereum client, and therefore most technical standards on Polygon are the same as for Ethereum. Furthermore full

compatibility with the Ethereum Virtual Machine (EVM) allows Ethereum smart contracts to be deployed on Polygon without modification.

The following applies to Optimism:

Optimism is a Layer 2 scaling solution built on Ethereum that uses Optimistic Rollups technology. Transactions are bundled outside the Ethereum main chain and only transmitted to Layer 1 in compressed form. This significantly reduces gas fees and increases transaction speed. Optimism is fully EVM-compatible and allows developers to migrate existing Ethereum smart contracts without major adjustments. Optimism's architecture is based on a modular rollup design, with data and execution layers treated separately to ensure scalability and flexibility.

The following applies to Arbitrum:

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

H.3 Technology used

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

The following applies to Ethereum Ether:

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

The following applies to Binance Smart Chain:

1. BSC-compatible wallets

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

2. Decentralised Ledger

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

3. BEP-20 token standard

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

4. Scalability and transaction efficiency

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

The following applies to Polygon POL:

Polygon operates as a decentralized ledger that records all token transactions on its network, ensuring transparency and security through an immutable record of transfers and ownership. To protect their holdings, users must securely manage their private keys and recovery phrases, since access to tokens depends entirely on these credentials.

The network relies on elliptic curve cryptography for secure transaction validation and execution. Polygon uses the secp256k1 curve with ECDSA for key generation and digital signatures, while the Keccak-256 hashing algorithm underpins address derivation and transaction integrity. This combination of cryptographic standards provides the foundation for both the security and reliability of the Polygon ecosystem.

Polygon's Bor client is based on Ethereum's Go Ethereum Client. Polygon's Heimdall client is built using Cosmos-SDK and CometBFT.

The following applies to Optimism:

Optimism is fully compatible with Ethereum (Layer 1) and uses the same development tools as Solidity, Vyper, and popular frameworks (Hardhat, Foundry, Truffle). This allows developers to deploy their applications on Optimism without making major changes. In addition, the bridge between Ethereum and Optimism is designed to allow assets to be easily transferred between the two networks.

The following applies to Arbitrum:

1. Arbitrum-compatible wallets: The tokens are supported by all wallets compatible with the Ethereum Virtual Machine (EVM), such as MetaMask.
2. Decentralised ledger: Arbitrum operates as a Layer-2 blockchain on Ethereum and maintains its own decentralised ledger for recording token transactions. Final transaction data is periodically posted to Ethereum Layer 1, ensuring long-term availability and resistance to tampering.
3. ERC-20 token standard: The Arbitrum network supports tokens implemented under the ERC-20 standard, the same as on Ethereum.
4. Arbitrum supports what is called "MultiVM", which is the combination of EVM support with a WASM-based virtual machine. The latter one being more efficient (lower gas costs) but specific to Arbitrum.
5. Scalability and transaction efficiency: As a rollup-based Layer-2, Arbitrum is intended to process higher volumes of transactions with lower fees compared to Ethereum Layer 1 by executing transactions off-chain and posting data on-chain using an optimistic rollup architecture.

H.4 Consensus mechanism

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

The following applies to Ethereum Ether:

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

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

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

3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates help ensure there is a sufficient pool of nodes ready to take on validation tasks, supporting network resilience and decentralisation.

Consensus process

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

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

6. Transaction finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the PoSA mechanism, which allows validators to reach consensus efficiently.

Security and economic incentives

7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to support honest behaviour. This staked amount can be slashed if validators act maliciously.

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

9. Transaction fees: BSC employs low transaction fees, paid in BNB. These fees are collected by validators as part of their rewards, incentivising them to validate transactions accurately and efficiently.

The following applies to Polygon POL:

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

Core Concepts

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

Consensus Process

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

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

The following applies to Optimism:

Since Optimism is based on Ethereum, it ultimately inherits its security via the Ethereum blockchain and the proof-of-stake consensus. Within the rollup system, Optimism relies on a "fault proof" procedure. By default, transactions are assumed to be correct ("optimistic"). Only in the event of suspected faults is a fault proof initiated, in which incorrect transactions can be challenged by challengers. This model allows for high efficiency while ensuring correctness.

The following applies to Arbitrum:

Arbitrum is a Layer-2 (L2) solution on Ethereum that is developed using the Arbitrum technology suite. L2 transactions do not have their own consensus mechanism and are only validated by the execution clients. The so-called sequencer regularly bundles stacks of L2 transactions and publishes

them on the L1 network, i.e. Ethereum. Ethereum's consensus mechanism (Proof-of-Stake) thus indirectly secures all L2 transactions as soon as they are written to L1.

H.5 Incentive mechanisms and applicable fees

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

The following applies to Ethereum Ether:

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

The following applies to Binance Smart Chain:

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

Incentive mechanisms

1. Validators: Staking rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. Selection process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks.

2. Delegators: Delegated staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. Shared rewards: Delegators earn a portion of the rewards that validators receive. This incentivises token holders to participate in the network's security and decentralisation by choosing reliable validators.

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

4. Economic Security: Slashing: Validators can be penalised for malicious behaviour or failure to perform their duties. Penalties can include slashing a portion of their staked tokens. Opportunity

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

Fees on the Binance Smart Chain

5. Transaction fees: Low fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are used to compensate validators. Dynamic fee structure: Transaction fees can vary based on network congestion and the complexity of transactions. However, BSC aims to keep fees significantly lower than those on the Ethereum mainnet.

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

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

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

The following applies to Polygon POL:

Incentive Mechanisms

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

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

3. Economic Security: Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions. Bond Requirements: Validators are required to bond a significant amount of POL tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity.

4. Transaction Fees: Low Fees: One of Polygon's main advantages is its low transaction fees compared to the Ethereum main chain. The fees are paid in POL tokens and are designed to be affordable to encourage high transaction throughput and user adoption. Dynamic Fees: Fees on Polygon can vary depending on network congestion and transaction complexity. However, they remain significantly lower than those on Ethereum, making Polygon an attractive option for users and developers.

5. Smart Contract Fees: Deployment and Execution Costs: Deploying and interacting with smart contracts on Polygon incurs fees based on the computational resources required. These fees are also paid in POL tokens and are much lower than on Ethereum, making it cost-effective for developers to build and maintain decentralized applications (dApps) on Polygon.

The following applies to Optimism:

Optimism charges significantly lower transaction fees than Ethereum Layer 1, as transactions are bundled in the rollup and written to the Ethereum main chain in compressed form. Gas fees on Optimism continue to be paid in ETH.

The incentive model is based on increased efficiency for users (lower fees, faster confirmation) and on the role of sequencers. Sequencers are central actors who collect, organize, and include transactions in the rollup. Their revenue comes from the gas fees they charge. Fault proofs ensure that sequencers cannot permanently enforce incorrect or malicious transactions. Fault proofs and their resolution are also incentivized economically to discourage faults to begin with.

The following applies to Arbitrum:

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

H.6 Use of distributed ledger technology

No – 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

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

Volatility: The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of

limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the crypto-asset at or close to a previously observed price, even where no negative project-specific event has occurred.

4. Counterparty and service provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG001FE242

S.3 Name of the cryptoasset

Kyber Network Crystal v2

S.4 Consensus Mechanism

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

The following applies to Ethereum Ether:

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

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

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

3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates help ensure there is a sufficient pool of nodes ready to take on validation tasks, supporting network resilience and decentralisation.

Consensus process

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

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

6. Transaction finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the PoSA mechanism, which allows validators to reach consensus efficiently.

Security and economic incentives

7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to support honest behaviour. This staked amount can be slashed if validators act maliciously.

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

9. Transaction fees: BSC employs low transaction fees, paid in BNB. These fees are collected by validators as part of their rewards, incentivising them to validate transactions accurately and efficiently.

The following applies to Polygon POL:

Polygon is a scaling solution for Ethereum that stores and process transaction data on its own separate chain and regularly submits checkpoints to Ethereum. This type of scaling solution is sometimes referred to as a plasma chain, and is distinct from sidechains, which don't store

checkpoints and Layer 2 solutions that store all transaction data on Ethereum in addition to the checkpoints. Here's a detailed explanation of how Polygon achieves consensus:

Core Concepts

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

Consensus Process

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

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

The following applies to Optimism:

Since Optimism is based on Ethereum, it ultimately inherits its security via the Ethereum blockchain and the proof-of-stake consensus. Within the rollup system, Optimism relies on a "fault proof" procedure. By default, transactions are assumed to be correct ("optimistic"). Only in the event of suspected faults is a fault proof initiated, in which incorrect transactions can be challenged by challengers. This model allows for high efficiency while ensuring correctness.

The following applies to Arbitrum:

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

S.5 Incentive Mechanisms and Applicable Fees

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

The following applies to Ethereum Ether:

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

The following applies to Binance Smart Chain:

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

Incentive mechanisms

1. Validators: Staking rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. Selection process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks.

2. Delegators: Delegated staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. Shared rewards: Delegators earn a portion of the rewards that validators receive. This incentivises token holders to participate in the network's security and decentralisation by choosing reliable validators.

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

4. Economic Security: Slashing: Validators can be penalised for malicious behaviour or failure to perform their duties. Penalties can include slashing a portion of their staked tokens. Opportunity cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing staked assets.

Fees on the Binance Smart Chain

5. Transaction fees: Low fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are used to compensate validators. Dynamic fee structure: Transaction fees can vary based on network congestion and the complexity of transactions. However, BSC aims to keep fees significantly lower than those on the Ethereum mainnet.

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

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

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

The following applies to Polygon POL:

Incentive Mechanisms

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

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

3. Economic Security: Slashing: Validators can be penalized through a process called slashing if they engage in malicious behavior or fail to perform their duties correctly. This includes double-signing or going offline for extended periods. Slashing results in the loss of a portion of the staked tokens, acting as a strong deterrent against dishonest actions. Bond Requirements: Validators are required to bond a significant amount of POL tokens to participate in the consensus process, ensuring they have a vested interest in maintaining network security and integrity.

4. Transaction Fees: Low Fees: One of Polygon's main advantages is its low transaction fees compared to the Ethereum main chain. The fees are paid in POL tokens and are designed to be affordable to encourage high transaction throughput and user adoption. Dynamic Fees: Fees on Polygon can vary depending on network congestion and transaction complexity. However, they remain significantly lower than those on Ethereum, making Polygon an attractive option for users and developers.

5. Smart Contract Fees: Deployment and Execution Costs: Deploying and interacting with smart contracts on Polygon incurs fees based on the computational resources required. These fees are also paid in POL tokens and are much lower than on Ethereum, making it cost-effective for developers to build and maintain decentralized applications (dApps) on Polygon.

The following applies to Optimism:

Optimism charges significantly lower transaction fees than Ethereum Layer 1, as transactions are bundled in the rollup and written to the Ethereum main chain in compressed form. Gas fees on Optimism continue to be paid in ETH.

The incentive model is based on increased efficiency for users (lower fees, faster confirmation) and on the role of sequencers. Sequencers are central actors who collect, organize, and include transactions in the rollup. Their revenue comes from the gas fees they charge. Fault proofs ensure that sequencers cannot permanently enforce incorrect or malicious transactions. Fault proofs and their resolution are also incentivized economically to discourage faults to begin with.

The following applies to Arbitrum:

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

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

2025-02-23

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

2026-02-23

S.8 Energy consumption

82.05887 kWh/a

S.9 Energy consumption sources and methodologies

The energy consumption associated with this crypto-asset is aggregated of multiple contributing components, primarily the underlying blockchain network and the execution of token-specific operations. To determine the energy consumption of a token, the energy consumption of the underlying blockchain network Ethereum Ether, Binance Smart Chain, Polygon POL, Optimism and Arbitrum is calculated first. A proportionate share of that energy use is then attributed to the token based on its expected 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

36.9016472538 %

S.11 Energy intensity

0.00001 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO₂e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.02731 tCO₂e/a

S.14 GHG intensity

0.00000 kgCO₂e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are 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 that are comparable in terms of their incentivization structure and consensus mechanism. This geolocation data is merged with public information from Our World in Data (see citation). The intensity is calculated as the marginal energy cost with respect to an additional transaction. Share of electricity generated by renewables – Ember and Energy Institute” [dataset]. Ember, “Yearly Electricity Data Europe”; Ember, “Yearly Electricity Data”; Energy Institute, “Statistical Review of World Energy” [original data]. Retrieved from <https://ourworldindata.org/grapher/share-electricity-renewables>.

S.16 Key GHG sources and methodologies

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

