CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG 42PHJB2BS

Preamble

00. Table of Content

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

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading 12
B.1 Issuer different from offeror or person seeking admission to trading 12
B.2 Name 12
B.3 Legal form 12
B4. Registered address 12
B.5 Head office 12
B.6 Registration date 12
B.7 Legal entity identifier 13
B.8 Another identifier required pursuant to applicable national law 13
B.9 Parent company 13
B.10 Members of the management body 13
B.11 Business activity 13
B.12 Parent company business activity 13
Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 13
C.1 Name 13
C.2 Legal form 13
C.3 Registered address 13
C.4 Head office 14
C.5 Registration date 14
C.6 Legal entity identifier 14
C.7 Another identifier required pursuant to applicable national law 14
C.8 Parent company 14
C.9 Reason for crypto-Asset white paper Preparation 14
C.10 Members of the Management body 14
C.11 Operator business activity 14
C.12 Parent company business activity 14
C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 14
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 14
Part D – Information about the crypto-asset project 14
D.1 Crypto-asset project name 14
D.2 Crypto-assets name 14
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 15
D.6 Utility Token Classification 16
D.7 Key Features of Goods/Services for Utility Token Projects 16
D.8 Plans for the token 16
D.9 Resource allocation 17
D.10 Planned use of Collected funds or crypto-Assets 18
Part E – Information about the offer to the public of crypto-assets or their admission to trading 18
E.1 Public offering or admission to trading 18
E.2 Reasons for public offer or admission to trading 18
E.3 Fundraising target 18
E.4 Minimum subscription goals 18
E.5 Maximum subscription goals 18
E.6 Oversubscription acceptance 18
E.7 Oversubscription allocation 18
E.8 Issue price 18
E.9 Official currency or any other crypto-assets determining the issue price 19
E.10 Subscription fee 19
E.11 Offer price determination method 19
E.12 Total number of offered/traded crypto-assets 19
E.13 Targeted holders 19
E.14 Holder restrictions 19
E.15 Reimbursement notice 19
E.16 Refund mechanism 19
E.17 Refund timeline 19
E.18 Offer phases 19
E.19 Early purchase discount 20
E.20 Time-limited offer 20
E.21 Subscription period beginning 20
E.22 Subscription period end 20
E.23 Safeguarding arrangements for offered funds/crypto- Assets 20
E.24 Payment methods for crypto-asset purchase 20
E.25 Value transfer methods for reimbursement 20
E.26 Right of withdrawal 20
E.27 Transfer of purchased crypto-assets 20

E.28 Transfer time schedule 20
E.29 Purchaser's technical requirements 20
E.30 Crypto-asset service provider (CASP) name 21
E.31 CASP identifier 21
E.32 Placement form 21
E.33 Trading platforms name 21
E.34 Trading platforms Market identifier code (MIC) 21
E.35 Trading platforms access 21
E.36 Involved costs 21
E.37 Offer expenses 21
E.38 Conflicts of interest 21
E.39 Applicable law 22
E.40 Competent court 22
Part F – Information about the crypto-assets 22
F.1 Crypto-asset type 22
F.2 Crypto-asset functionality 22
F.3 Planned application of functionalities 23
A description of the characteristics of the crypto asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article 24
F.4 Type of crypto-asset white paper 24
F.5 The type of submission 24
F.6 Crypto-asset characteristics 24
F.7 Commercial name or trading name 24
F.8 Website of the issuer 24
F.9 Starting date of offer to the public or admission to trading 24
F.10 Publication date 24
F.11 Any other services provided by the issuer 24
F.12 Language or languages of the crypto-asset white paper 24
F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates 25
F.14 Functionally fungible group digital token identifier 25
F.15 Voluntary data flag 25
F.16 Personal data flag 25
F.17 LEI eligibility 25
F.18 Home Member State 25
F.19 Host Member States 25

Part G – Information on the rights and obligations attached to the crypto-assets 25
G.1 Purchaser rights and obligations 25
G.2 Exercise of rights and obligations 25
G.3 Conditions for modifications of rights and obligations 26
G.4 Future public offers 26
G.5 Issuer retained crypto-assets 26
G.6 Utility token classification 26
G.7 Key features of goods/services of utility tokens 26
G.8 Utility tokens redemption 26
G.9 Non-trading request 26
G.10 Crypto-assets purchase or sale modalities 26
G.11 Crypto-assets transfer restrictions 26
G.12 Supply adjustment protocols 27
G.13 Supply adjustment mechanisms 27
G.14 Token value protection schemes 27
G.15 Token value protection schemes description 27
G.16 Compensation schemes 27
G.17 Compensation schemes description 27
G.18 Applicable law 27
G.19 Competent court 27
Part H – information on the underlying technology 27
H.1 Distributed ledger technology (DTL) 27
H.2 Protocols and technical standards 28
H.3 Technology used 30
H.4 Consensus mechanism 31
H.5 Incentive mechanisms and applicable fees 33
H.6 Use of distributed ledger technology 34
H.7 DLT functionality description 34
H.8 Audit 34
H.9 Audit outcome 34
Part I – Information on risks 34
I.1 Offer-related risks 34
I.2 Issuer-related risks 36
I.3 Crypto-assets-related risks 38
I.4 Project implementation-related risks 40
I.5 Technology-related risks 40

I.6 Mitigation measures 42

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts 43

J.1 Adverse impacts on climate and other environment-related adverse impacts 43

S.1 Name 43

S.2 Relevant legal entity identifier 43

S.3 Name of the cryptoasset 43

S.4 Consensus Mechanism 43

S.5 Incentive Mechanisms and Applicable Fees 44

S.6 Beginning of the period to which the disclosure relates 46

S.7 End of the period to which the disclosure relates 46

S.8 Energy consumption 46

S.9 Energy consumption sources and methodologies 46

S.10 Renewable energy consumption 46

S.11 Energy intensity 46

S.12 Scope 1 DLT GHG emissions – Controlled 46

S.13 Scope 2 DLT GHG emissions – Purchased 46

S.14 GHG intensity 46

S.15 Key energy sources and methodologies 46

S.16 Key GHG sources and methodologies 47

01. Date of notification

This white paper was notified at 2026-01-06.

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 XRP tokens referred to in this white paper are crypto-assets other than EMTs and ARTs, and are issued on the XRP Ledger (2025-10-16 and according to DTI FFG shown in F.14) with a total number of 100,000,000,000 XRP. The first activity on the XRP Ledger can be identified at ledger (block) #32 570, which represents the earliest available ledger following the loss of ledgers #1 to #32 569 (see: https://xrpscan.com/ledger/32570). All XRP was created along with the ledger itself at genesis, and no further XRP can be minted thereafter.

The crypto-asset XRP is the native crypto-asset of the XRP Ledger (XRPL), a public, open-source layer-1 blockchain intended for fast, low-cost value transfer and settlement, including cross-border payments and exchange between different assets on the ledger. XRP is primarily used to pay network transaction fees (with a small amount of XRP irrevocably destroyed per transaction to help deter spam) and can act as a bridge asset to support liquidity-efficient exchange between different currencies or tokens on XRPL's built-in exchange functionality.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

federal state Hamburg.

A.4 Head office

Crypto Risk Metrics GmbH has no head office.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider, which supports regulated entities in the fulfilment of their regulatory requirements. In this regard, Crypto Risk Metrics GmbH, among other services, acts as a data-provider for ESG data according to article 66 (5). Due to the regulations laid out in article 4 (7), 5 (4) and 66 (3) of the Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, Crypto Risk Metrics GmbH aims to provide central services for crypto-asset white papers.

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): negative EUR 50.891,81

2023 (unaudited): negative EUR 27.665,32

2022: EUR 104.283,00.

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

Ripple Labs Inc. is the company most closely associated with the creation and ongoing development of the XRP Ledger and the XRP crypto-asset. Publicly available sources and historical documentation indicate that the XRP Ledger (XRPL) was initially developed by engineers David Schwartz, Jed McCaleb, and Arthur Britto in 2011, and that shortly thereafter, in 2012, they co-founded OpenCoin (later renamed Ripple Labs Inc.) together with Christian Larsen.

B.3 Legal form

The legal form of Ripple Labs Inc. is XTIQ, which corresponds to "Corporation".

B4. Registered address

The registered address of Ripple Labs Inc. Is US-DE, 1209 Orange St, Corporation Trust Center, Wilmington, DE 19801,

United States of America,

US-DE

B.5 Head office

The head office of Ripple Labs Inc. Is US-CA, 600 Battery St, San Francisco, CA 94111.

United States of America

US-CA

B.6 Registration date

2014-09-15

B.7 Legal entity identifier

9845001L01C142EE4094

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Identity	Function	Business Address
Brad Garlinghouse	CEO	1209 Orange St, Corporation Trust Center, Wilmington, DE 19801, USA
David Schwartz	CTO	1209 Orange St, Corporation Trust Center, Wilmington, DE 19801, USA
Monica Long	President	1209 Orange St, Corporation Trust Center, Wilmington, DE 19801, USA
Stuart Alderoty	CLO	1209 Orange St, Corporation Trust Center, Wilmington, DE 19801, USA
Chris Larsen	Executive Chairman	1209 Orange St, Corporation Trust Center, Wilmington, DE 19801, USA

B.11 Business activity

Ripple Labs Inc.: Responsible for operating and maintaining user interfaces and related legal, compliance, and contractual matters for the XRP Ledger ecosystem.

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: "Ripple XRP", Short Name: "XRP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-10-16).

D.2 Crypto-assets name

Long Name: "Ripple XRP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-10-16).

D.3 Abbreviation

Short Name: "XRP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-10-16).

D.4 Crypto-asset project description

According to public information (source: https://xrpl.org/docs, accessed 2025-10-16), XRP is the native digital asset of the XRP Ledger (XRPL), a decentralized and open-source distributed ledger intended to provide a fast, efficient, and scalable infrastructure for the transfer of value. The XRP Ledger operates on a consensus protocol known as the XRP Ledger Consensus Protocol (XRPLCP), which enables participating validators to agree on the validity and order of transactions without relying on mining or proof-of-stake. Consensus is reached through iterative rounds of validation among independently operated nodes, based on overlapping sets of trusted validators known as Unique Node Lists (UNLs). A ledger version is considered final once at least 80 % of trusted validators agree on its contents.

All XRP in existence - 100 billion units - were created at the inception of the ledger in 2012. The supply is finite, and no additional XRP can be minted. XRP is divisible to six decimal places, with one million drops equaling one XRP. A small amount of XRP is irreversibly destroyed (“burned”) with each transaction as an anti-spam mechanism, ensuring long-term scarcity.

Within the XRP Ledger, XRP serves three primary functions. First, it acts as the native medium of exchange for settling peer-to-peer transactions and cross-currency payments. Second, it is required as a reserve to activate ledger accounts and maintain trust lines, preventing network abuse through excessive account creation. Third, it provides liquidity and serves as the base asset for path-finding and exchange functions within the ledger’s built-in decentralized exchange.

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

Type of person	Name of person	Business address of person	Domicile of company
Other person involved in implementation	David Schwartz	Can not be found	Can not be found
Other person involved in implementation	Jed McCaleb	Can not be found	Can not be found
Other person involved in implementation	Monica Long	Can not be found	Can not be found
Other person involved in implementation	Brad Garlinghouse	Can not be found	Can not be found
	Arthur Britto	Can not be found	

Type of person	Name of person	Business address of person	Domicile of company
Other person involved in implementation			Can not be found
Other person involved in implementation	Christian Larsen	Can not be found	Can not be found
Other person involved in implementation	Ripple Labs Inc.	US-DE, 1209 Orange St, Wilmington, DE 19801, United States	United States
Other person involved in implementation	XRP Ledger Foundation	60 Rue François Ier, 75008 Paris, France	France

D.6 Utility Token Classification

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

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

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

D.8 Plans for the token

The XRP Ledger (XRPL) and its native token, XRP, have evolved through several major development stages since their inception. The following overview summarizes past milestones and publicly communicated future plans, according to the official project documentation and whitepapers (https://xrpl.org/about/history, accessed 2025-10-16).

Past Milestones:

The XRP Ledger was first developed between 2011 and 2012 by engineers David Schwartz, Jed McCaleb, and Arthur Britto, who sought to create a more energy-efficient and scalable alternative to Bitcoin. The network officially launched in June 2012, introducing XRP as its native digital asset. Later that year, Christian Larsen joined the team, and the company was incorporated first as NewCoin in September 2012, renamed OpenCoin and subsequently Ripple Labs Inc. in 2013.

In 2020, the independent, non-profit XRPL Foundation was established (formally MTU XRP Ledger Trust) to promote open-source development and ecosystem adoption. It received initial donations from Coil, Ripple, and Gatehub and supports network research, validator diversity, and community-driven governance initiatives.

The XRP Ledger Consensus Protocol (XRP LCP), described in Ripple Labs' 2014 white paper and analyzed by Ripple Research in 2018 ("Analysis of the XRP Ledger Consensus Protocol," Chase & MacBrough), established a low-latency Byzantine-fault-tolerant consensus model relying on Unique Node Lists (UNLs) rather than mining. This protocol has remained the operational backbone of the ledger. Since 2017, XRP's supply management has been governed by a series of on-ledger escrows totaling 55 billion XRP, ensuring a predictable monthly release schedule of up to 1 billion XRP, with unreleased amounts re-escrowed (see https://ripple.com/insights/explanation-ripples-xrp-escrow/).

Future milestones:

According to publicly available information ("The Next Phase of Institutional DeFi on XRPL," Ripple Team, 2025-09-22), ongoing development focuses on extending XRPL's compliance and institutional-finance capabilities. Upcoming releases include a native lending protocol (based on specifications XLS-65/66) and expanded Multi-Purpose Token (MPT) functionality enabling complex financial instruments such as bonds and structured products to be represented directly on-chain.

Further milestones involve the integration of zero-knowledge proofs (ZKPs) for privacy-preserving transactions and confidential MPTs, targeted for Q1 2026.

Parallel efforts concentrate on enhancing decentralization through a more diversified validator ecosystem and improved UNL governance. In the longer term, the research-backed Cobalt consensus protocol (Ripple Research 2018) remains a candidate to replace the existing XRP LCP.

No fixed roadmap specifying versioned releases or timelines has been formally published. The achievement of the described milestones depends on technical implementation, validator approval, and evolving market and regulatory conditions. Therefore, no assurance can be given that all initiatives will be completed as planned or that their implementation will not have adverse consequences for XRP holders.

D.9 Resource allocation

The development, maintenance and broader ecosystem support of the XRP Ledger and the crypto-asset XRP are underpinned by financial and organisational resources originating primarily from Ripple and entities affiliated with its ecosystem. Since inception, the project has been supported through multiple private financing rounds involving institutional and professional investors, including venture capital firms, strategic corporate investors and other qualified market participants.

Publicly available disclosures indicate that Ripple has conducted several funding rounds over time, reflecting sustained external financial support for the continued operation, technical development and ecosystem expansion related to XRP and the XRP Ledger. The most recent disclosed financing round took place in 2025 and reportedly resulted in the raising of more than USD 500 million from

a consortium of well-known venture capital and institutional investors, following a series of earlier investment rounds in preceding years.

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

The white paper concerns the admission to trading (i. e. ATTR).

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The total supply of the crypto-asset is set at 100,000,000,000 units. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

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

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

Crypto Risk Metrics GmbH has established, implemented, and documented comprehensive internal policies and procedures for the identification, prevention, management, and documentation of conflicts of interest in accordance with applicable regulatory requirements. These internal measures are actively applied within the organisation. For the purposes of this specific assessment and the

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

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

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

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

F.2 Crypto-asset functionality

According to the official documentation (https://xrpl.org/ and https://xrpl.org/docs, accessed 2025-10-15), XRP represents the native crypto-asset of the XRP Ledger (XRPL), an open-source, decentralized blockchain protocol optimized for high-speed, low-cost transactions and institutional-grade financial use cases. It functions as the core utility asset of the XRPL, enabling the settlement and validation of transactions within the network.

The primary uses of XRP include: (i) serving as the native currency required to pay transaction fees ("gas") and to maintain reserve balances for activating ledger accounts; (ii) acting as a bridge asset in cross-currency and cross-border payments, allowing direct settlement between different fiat or digital currencies without intermediaries; and (iii) providing liquidity within decentralized exchange (DEX) and automated market-maker (AMM) functions native to the XRPL protocol.

XRP is integral to the operation of the XRP Ledger Consensus Protocol (XRP LCP), a Byzantine fault-tolerant mechanism through which network validators agree on the transaction set to be applied to each ledger version. This consensus process ensures network integrity and prevents double spending without relying on mining or staking. Each new ledger version contains the entire current state, so participants can verify account balances and transactions independently without reconstructing the full history.

Unlike issued tokens on the XRPL, all XRP was created at the ledger's inception, and no additional units can ever be minted. XRP does not grant holders any ownership, profit-sharing, redemption, or equity rights in Ripple Labs Inc. or any other entity. Its utility and value derive solely from its use within the XRPL network and its adoption in payment and liquidity applications.

All described functionalities depend on the continued operation and governance of the XRP Ledger protocol. Their effectiveness and availability are subject to validator participation, network conditions, and ongoing technical development, and cannot be independently guaranteed.

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

F.3 Planned application of functionalities

Future Plans:

According to publicly available information ("The Next Phase of Institutional DeFi on XRPL," Ripple Team, 2025-09-22), ongoing development focuses on extending XRPL's compliance and institutional-finance capabilities. Upcoming releases include a native lending protocol (based on specifications XLS-65/66) and expanded Multi-Purpose Token (MPT) functionality enabling complex financial instruments such as bonds and structured products to be represented directly on-chain.

Further milestones involve the integration of zero-knowledge proofs (ZKPs) for privacy-preserving transactions and confidential MPTs, targeted for Q1 2026.

Parallel efforts concentrate on enhancing decentralization through a more diversified validator ecosystem and improved UNL governance. In the longer term, the research-backed Cobalt consensus protocol (Ripple Research 2018) remains a candidate to replace the existing XRP LCP.

No fixed roadmap specifying versioned releases or timelines has been formally published. The achievement of the described milestones depends on technical implementation, validator approval, and evolving market and regulatory conditions. Therefore, no assurance can be given that all initiatives will be completed as planned or that their implementation will not have adverse consequences for XRP holders.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

The tokens are crypto-assets other than EMTs and ARTs, which are available on the XRP Ledger blockchain. The tokens are fungible (up to 6 digits after the decimal point). A total of 100,000,000,000 units have been issued. 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: "Ripple XRP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-10-16).

F.8 Website of the issuer

https://ripple.com/

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

2026-02-04

F.10 Publication date

2026-02-04

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

L6GTZC9G4; J815X0DG2; F2FP5N8RD

F.14 Functionally fungible group digital token identifier

42PHJB2BS

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

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

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

G.2 Exercise of rights and obligations

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

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

G.3 Conditions for modifications of rights and obligations

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

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

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

G.4 Future public offers

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

G.5 Issuer retained crypto-assets

Ripple publicly reports its retained XRP in two categories (XRP held in wallets and XRP subject to on-ledger escrow): as of 2025-07-31, Ripple reports 4,740,364,374 XRP held in its wallets and 35,900,000,005 XRP subject to on-ledger escrow, i.e., 40,640,364,379 XRP retained in total (≈40.6% of the 100 billion maximum supply). Source: https://ripple.com/xrp/, accessed 2025-12-22.

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 2025-12-03.

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

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 100,000,000,000 tokens. Investors should note that changes in the token supply can have a negative impact.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

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

H.2 Protocols and technical standards

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

The following applies to XRP Ledger:

The XRPL architecture is based on a peer-to-peer network of nodes running the “rippled” server software, which performs transaction validation and consensus.

The protocol defines standardized transaction and ledger object types, such as payments, trust-line management, decentralized exchange operations, escrows, and automated market-maker functionalities. All network upgrades are introduced through a formal amendment process, under which validators vote to activate new features. Once a qualified majority threshold is achieved, the protocol automatically enforces the new rules.

Ledger states are represented through authenticated hash trees (SHAMaps) that guarantee integrity and allow any participant to verify a ledger’s correctness using cryptographic proofs. Each validated ledger contains a complete snapshot of the current state and a reference to its predecessor. Because the full state is included in every ledger, new nodes can synchronize from recent validated states without reconstructing the entire transaction history.

Cross-currency payments on XRPL use atomic path-finding and on-ledger order books to facilitate deterministic settlement between multiple assets.

The following applies to Ethereum:

The crypto-asset operates on a well-defined set of protocols and technical standards that are intended to ensure its security, decentralization, and functionality. 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 utilizes a Proof-of-Staked Authority (PoSA) consensus mechanism. This mechanism combines elements of Proof-of-Authority (PoA) and Proof-of-Stake (PoS) and is intended to secure the network and validate transactions. In PoSA, validators are selected based on their stake and authority, with the goal of providing fast transaction times and low fees while maintaining network security through staking.

H.3 Technology used

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

The following applies to Ripple:

1. The XRP Ledger functions as a decentralized, open-source ledger that records all transactions and balances in a public, verifiable, and tamper-resistant manner. Each validated ledger contains a complete snapshot of the network's state, ensuring transparency and auditability of all token transfers and ownership records.

2. Private Key Management: Access to funds and control over accounts on the XRP Ledger are secured through cryptographic private keys held solely by users. Wallets use private keys to sign transactions, which are then broadcast and validated by the network. The protection of these private keys and recovery phrases remains the responsibility of the user and is essential to prevent unauthorized access.

3. Cryptographic Integrity: The XRP Ledger uses elliptic curve cryptography based on the secp256k1 and ed25519 curves to generate digital signatures and validate transactions. Data integrity is maintained through cryptographic hashing, using the SHA-512Half algorithm to produce transaction and ledger identifiers. These cryptographic standards ensure the authenticity, non-repudiation, and security of all transactions.

4. Blockchain Scalability: Each new ledger is finalized approximately every three to five seconds, and the network can process up to 1,500 transactions per second under optimal conditions. Since each ledger contains the full current state, new nodes can synchronize quickly without replaying the entire historical transaction log.

5. Consensus: The XRP Ledger employs the XRP Ledger Consensus Protocol. Validators on the network exchange transaction proposals and reach agreement when at least 80% of trusted nodes (the Unique Node List) approve the same transaction set. This process provides fast, energy-efficient finality and ensures that all participants maintain an identical view of the ledger within seconds.

The following applies to Ethereum:

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. Ledger

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

3. BEP-20 Token Standard

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

4. Scalability and Transaction Efficiency

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

H.4 Consensus mechanism

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

The following applies to XRP Ledger:

The XRP Ledger uses a deterministic consensus algorithm designed to achieve Byzantine fault-tolerant agreement without relying on mining or staking. Each server maintains its own Unique Node List (UNL), representing a subset of validators that it trusts to behave honestly. During each consensus round, validators exchange proposals regarding the set of candidate transactions to

apply to the previous ledger. Through successive rounds of voting and proposal adjustment, consensus is reached when at least 80% of the trusted validators agree on the same transaction set and resulting state. The system tolerates up to twenty percent of validator faults or communication failures without halting progress.

The following applies to Ethereum:

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

The following applies to 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 ensures fast block times and low fees while maintaining a level of decentralization and security. Core Components 1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security. 2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security. 3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process 4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes. 5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network. 6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives 7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB. 8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network’s security. Validators and delegators share transaction fees as rewards, which provides continuous

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

H.5 Incentive mechanisms and applicable fees

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

The following applies to XRP Ledger:

Transaction cost in XRPL is expressed as XRP destroyed (i.e. burned) when the transaction is validated. The foundational cost is 10 drops (0.00001 XRP) for a minimal transaction. Under network load, this cost can scale upward. The XRP Ledger does not employ traditional block-based rewards.

In addition to transaction costs, each ledger account must maintain a minimum reserve balance denominated in XRP. The base reserve is 1 XRP, with an additional incremental reserve of 0.2 XRP per owned object such as offers, escrows, or trust lines.

Fee and reserve settings evolve via fee voting by validators. Every ~15 minutes, validators signal preferred values, contributing to a consensus median that determines the network-wide base fee, reserve base, and incremental reserve.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators. Incentive Mechanisms 1. Validators: Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks. 2. Delegators: Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in

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

H.6 Use of distributed ledger technology

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

H.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service-provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

7. Open, Unresolved and Historical Legal Proceedings

Certain legal persons and natural persons associated with the development, promotion or broader ecosystem of the crypto-asset XRP have, in the past, been involved in legal and regulatory proceedings with supervisory and enforcement authorities in various jurisdictions. These proceedings have included, disputes with financial market regulators concerning the legal classification, distribution and regulatory treatment of XRP.

While some of these proceedings have been resolved through settlements or court decisions, including publicly reported outcomes, such resolutions do not preclude the possibility that additional legal or regulatory matters may exist that are not publicly disclosed, are ongoing, or may arise in the future. Furthermore, interpretations of applicable laws and regulatory frameworks may evolve over time, potentially giving rise to new investigations, enforcement actions or litigation.

Future legal or regulatory proceedings, whether related to past conduct or new developments, could result in financial penalties, operational restrictions, reputational damage, changes to business models, or other adverse consequences. Such outcomes may have a negative impact on the development, availability, utility, market perception and value of the crypto-asset XRP and could therefore adversely affect holders or prospective investors.

No assurance can be given that further legal disputes or regulatory actions will not occur, nor that any such matters would be resolved favourably. Investors should carefully consider these legal and regulatory risks when assessing the crypto-asset.

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the cryptoasset

Ripple XRP

S.4 Consensus Mechanism

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

The following applies to XRP Ledger:

The XRP Ledger uses a deterministic consensus algorithm designed to achieve Byzantine fault-tolerant agreement without relying on mining or staking. Each server maintains its own Unique Node List (UNL), representing a subset of validators that it trusts to behave honestly. During each consensus round, validators exchange proposals regarding the set of candidate transactions to apply to the previous ledger. Through successive rounds of voting and proposal adjustment, consensus is reached when at least 80% of the trusted validators agree on the same transaction set and resulting state. The system tolerates up to twenty percent of validator faults or communication failures without halting progress.

The following applies to Ethereum:

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

The following applies to 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 ensures fast block times and low fees while maintaining a level of decentralization and

security. Core Components 1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security. 2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security. 3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process 4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes. 5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network. 6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives 7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB. 8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network’s security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance. 9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

S.5 Incentive Mechanisms and Applicable Fees

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

The following applies to XRP Ledger:

Transaction cost in XRPL is expressed as XRP destroyed (i.e. burned) when the transaction is validated. The foundational cost is 10 drops (0.00001 XRP) for a minimal transaction. Under network load, this cost can scale upward. The XRP Ledger does not employ traditional block-based rewards.

In addition to transaction costs, each ledger account must maintain a minimum reserve balance denominated in XRP. The base reserve is 1 XRP, with an additional incremental reserve of 0.2 XRP per owned object such as offers, escrows, or trust lines.

Fee and reserve settings evolve via fee voting by validators. Every ~15 minutes, validators signal preferred values, contributing to a consensus median that determines the network-wide base fee, reserve base, and incremental reserve.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

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

2024-12-15

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

2025-12-15

S.8 Energy consumption

456261.38601 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 XRP Ledger, Ethereum and BNB Smart Chain is calculated first. A proportionate share of that energy use is then attributed to the token based on its activity level within the network (e.g. transaction volume, contract execution).

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

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

S.10 Renewable energy consumption

39.5998987240 %

S.11 Energy intensity

0.00002 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

152.84868 tCO2e/a

S.14 GHG intensity

0.00001 kgCO2e

S.15 Key energy sources and methodologies

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

S.16 Key GHG sources and methodologies

To determine the GHG Emissions, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their 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.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.