CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG GWM30MLW3

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified on 2026-09-01.

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

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

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

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

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

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

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

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

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

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

Summary

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

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

08. Characteristics of the crypto-asset

The crypto-asset Cronos (CRO) referred to in this white paper is a crypto-asset other than an e-money token (EMT) or an asset-referenced token (ART). The supply of the crypto-asset is limited to 100,000,000,000 units. The first on-chain activity of the crypto-asset occurred on 2018-11-14 on Ethereum (transaction hash: 0xbd29dfc2cfc9b2e2170d6a564903c3e32e713b61c01e31ff8664cca24736b431, source: https://etherscan.io/tx/0xbd29dfc2cfc9b2e2170d6a564903c3e32e713b61c01e31ff8664cca24736b431, accessed on 2026-07-30). The first activity of the crypto-asset on the Cronos PoS chain occurred on 2021-03-25 (block hash: 5BADB996831CE0C37BA3ED50C03E12400B97D6B8DA19E932FADCD62E91A97FEA, source: https://cronos-pos.org/explorer/block/1, accessed on 2026-07-30). The first activity of the crypto-asset on the Cronos EVM chain occurred on 2021-11-08 (block hash: 0xa7f4e603aa51239a15e0a3fafb15c6e4c6d6f2c39c55770330efd2fa5afc12a9, source: https://explorer.cronos.org/block/1, accessed on 2026-07-30). The first activity of the relevant CRO-related IBC channel between Cronos POS and Cosmos Hub can be viewed on 2021-07-30 (channel: CRONOS POS/channel-27 – COSMOS HUB/channel-187, source: https://www.mintscan.io/cosmos/relayers/channel-187/crypto-org/channel-27, accessed 2026-08-06). The first activity of the relevant CRO-related IBC channel between Osmosis and Cronos POS can be viewed on 2021-06-19 (channel: OSMOSIS/channel-5 – CRONOS POS/channel-10, source: https://www.mintscan.io/osmosis/relayers/channel-5/crypto-org/channel-10, accessed 2026-08-06). The first on-chain activity of the crypto-asset occurred on 2021-12-25 on Solana (transaction signature: 2mME2CJWPd3rJerQNQT63Vuy4oA53oFcri2WqWgH1ePYAaDAb4Q7QcQ97LKJkrGXGX3kYJn64915DLvNiWqhvRcz, source: https://solscan.io/tx/2mME2CJWPd3rJerQNQT63Vuy4oA53oFcri2WqWgH1ePYAaDAb4Q7QcQ97LKJkrGXGX3kYJn64915DLvNiWqhvRcz, accessed on 2026-08-06). The crypto-asset was not natively issued on the Cronos zkEVM, a Layer-2 network on which transaction fees were paid in a separate derivative asset rather than in CRO. That network is being wound down and holders of assets on it have been directed to transfer them off it by 2027-06-03, after which access to those assets may be limited. Representations of the crypto-asset on networks other than the Cronos POS Chain arise from bridging arrangements, which may be operated by third parties and are not necessarily established or maintained by any person connected with the crypto-asset project. The activity records above reflect the first recorded activity on each network and do not indicate that any such network or bridging arrangement remains in active use at the date of this white paper.

According to publicly available information (source: https://cronos.com/, accessed 2026-07-30), Cronos is a blockchain network on which trading in crypto-assets, tokenised equities and prediction markets is intended to settle on a shared ledger. The network comprises two production chains: the Cronos POS Chain, which is the settlement and governance layer on which CRO is natively issued, and the Cronos EVM, an Ethereum-compatible chain for smart contracts and decentralised applications. The project's principal user-facing product is the Cronos App, a mobile trading application. A third network, the Cronos zkEVM, is being wound down and development effort has been consolidated on the Cronos EVM. Ecosystem funding, accelerator programmes and infrastructure support are provided by organisations connected to the project. These activities do not constitute any assurance as to adoption, performance or continued operation of the network or its products.

CRO, formerly known as Crypto.org Coin, is the native asset of the Cronos POS Chain. Validators bond CRO to participate in block production and transaction validation, and delegators may bond CRO to validators, in each case receiving protocol-level staking rewards. Bonded CRO also carries participation in protocol-level governance on that chain. On the Cronos EVM, CRO is the transaction fee (gas) asset for smart-contract execution and carries no staking or governance function. CRO is also issued in bridged form on other networks for compatibility and liquidity purposes.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

federal state of Hamburg.

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

FORIS DAX, INC.

B.3 Legal form

The legal form of FORIS DAX, INC. is XTIQ, which corresponds to "Corporation".

B.4 Registered address

The registered address of FORIS DAX, INC. is c/o Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808,

United States,

US-DE

B.5 Head office

The head office of FORIS DAX, INC. is 110 N College Ave, Suite 500, Tyler, TX 75702,

United States,

US-TX

B.6 Registration date

FORIS DAX, INC. was registered on 2020-01-16.

B.7 Legal entity identifier

The Legal Entity Identifier (LEI) of FORIS DAX, INC. is 984500067C5147A95C80.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Foris Holdings US, Inc.

B.10 Members of the management body

Name	Position	Business address
James H. Grabow	Board Member	110 N College Ave, Suite 500, Tyler, TX 75702
Antonio Alvarez Lorenzo	COO	110 N College Ave, Suite 500, Tyler, TX 75702

B.11 Business activity

FORIS DAX, INC. (Crypto.com) operates as a global provider of cryptocurrency exchange, wallet, payment, and financial service products. Its activities broadly include offering trading services for digital assets, developing custodial and non-custodial wallet solutions, and supporting payment use cases through its mobile application, card programs, and related infrastructure. The group operates through multiple licensed subsidiaries across various jurisdictions. The CRO token (formerly known as Crypto.org Coin) functions as the central functional token of the Crypto.com ecosystem. It is designed to support technical, economic, and coordination mechanisms across two primary blockchain networks:

- Cronos PoS Chain (proof-of-stake settlement and governance layer),

- Cronos EVM Layer-1 (smart-contract execution compatible with Ethereum tooling).

B.12 Parent company business activity

Could not be found while drafting this white paper.

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: "Cronos", Short Name: "CRO" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-07-30).

D.2 Crypto-assets name

Long Name: "Cronos" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-07-30).

D.3 Abbreviation

Short Name: "CRO" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-07-30).

D.4 Crypto-asset project description

According to publicly available information (sources: https://cronos.com/network, https://cronos.com/about-cro, https://docs.cronos.com/, accessed 2026-08-06), Cronos is a blockchain project which positions itself as a settlement layer for stablecoins and tokenised assets, on which trading in crypto-assets, tokenised equities and prediction markets is intended to settle on a shared ledger. Integrations with stablecoin issuance, custody, node infrastructure and blockchain analytics providers are described as supporting institutional use of the network.

The project comprises two production blockchain networks. The Cronos POS Chain is the network on which CRO is natively issued and which is secured by a proof-of-stake consensus mechanism, and it is the network on which protocol-level governance for that chain is conducted. The Cronos EVM is a Layer-1 network compatible with the Ethereum Virtual Machine, on which smart contracts and decentralised applications are deployed permissionlessly using established Ethereum development tooling. Participation in block production on that network is not permissionless: the validator set is admitted by invitation and applications are not open (source: https://docs.cronos.com/cronos-chain-protocol/cronos-general-faq, accessed 2026-08-31). The two networks are interoperable and CRO is also issued in bridged form on other blockchain networks for compatibility and liquidity purposes.

A third network, the Cronos zkEVM, is being wound down. It is a Layer-2 network secured via Ethereum which used a derivative asset rather than CRO to pay transaction fees. The network remains in operation at the date of this white paper. Development effort has been consolidated on the Cronos EVM, and holders of assets on the Cronos zkEVM have been directed to transfer them (source: https://docs-zkevm.cronos.com/for-users/cronos-zkevm-bridge, accessed 2026-08-06) off that network by 2027-06-03, after which access to those assets may be limited.

The project's principal user-facing product is the Cronos App, a self-custody application for trading crypto-assets, equities and prediction markets. The project further states that revenue generated by the Cronos App is intended to be applied to staking rewards, purchases of CRO and reductions of supply. No assurance is given as to whether, when or in what form the Cronos App or those revenue arrangements will become operational.

Development, funding and adoption of the network are supported by organisations connected to the project, through funding initiatives, accelerator programmes, infrastructure provision and ecosystem coordination. These activities do not constitute any assurance as to the level of adoption, the performance or the continued operation of the network or its products.

The CRO crypto-asset does not grant ownership rights, profit-participation claims, or legal entitlements in relation to any issuing or supporting entity. Its role is limited to technical and functional use within the Cronos networks, being transaction execution on the Cronos POS Chain and the Cronos EVM, and staking-based participation in network security and in protocol-level governance on the Cronos POS Chain. The availability and scope of these functionalities may evolve over time and remain subject to protocol upgrades, governance decisions, validator participation, changes to the networks on which the crypto-asset is used, and broader technical, economic and regulatory considerations.

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

Name of person	Type of person	Business address of person	Domicile of company
Kris Marszalek	Other person involved in implementation	128 Beach Road, #27-03 Guoco Midtown Office, 189773	Singapore
Rafael Melo (Rafael de Marco e Melo)	Other person involved in implementation	128 Beach Road, #27-03 Guoco Midtown Office, 189773	Singapore
Bobby Bao	Other person involved in implementation	108 W. 13th Street, Suite 100, Wilmington, DE 19801	United States
Gary Or (Ping Lam Or)	Other person involved in implementation	128 Beach Road, #27-03 Guoco Midtown Office, 189773	Singapore
Eric Anziani	Other person involved in implementation	128 Beach Road, #27-03 Guoco Midtown Office, 189773	Singapore
Mariana Dinkova Kushev	Other person involved in implementation	Level 7, Spinola Park, Triq Mikiel Ang Borg, SPK 1000 St. Julians	Malta
Ken Timsit	Other person involved in implementation	108 W. 13th Street, Suite 100, Wilmington, DE 19801	United States
Edward Adlard	Other person involved in implementation	108 W. 13th Street, Suite 100, Wilmington, DE 19801	United States
Ang Chin Tah	Other person involved in implementation	128 Beach Road, #27-03 Guoco Midtown Office, 189773	Singapore
Cronos Labs Inc.	Other person involved in implementation	108 W. 13th Street, Suite 100, Wilmington, DE 19801	United States
Foris DAX MT Limited	Other person involved in implementation	Level 7, Spinola Park, Triq Mikiel Ang Borg, SPK 1000 St. Julians	Malta
Foris DAX Trust Company, LLC	Other person involved in implementation	10 Ferry Street, Suite 313, Concord, NH 03301	United States

Name of person	Type of person	Business address of person	Domicile of company
Foris DAX Holdings Limited	Other person involved in implementation	Suite Nos. 5-7A, 17/F, Pacific Plaza, 410 Des Voeux Road W, Hong Kong 000000, Hong Kong	Hong Kong
Foris DAX Limited	Other person involved in implementation	94 Solaris Avenue, P.O. Box 1348, Grand Cayman, c/o Mourant Governance Services (Cayman) Limited, KY1-1108	Cayman Islands
Foris DAX Asia Pte. Ltd.	Other person involved in implementation	128 Beach Road, #27-03 Guoco Midtown Office, 189773	Singapore
Matt David	Other person involved in implementation	Suite Nos. 5-7A, 17/F, Pacific Plaza, 410 Des Voeux Road W, Hong Kong 000000, Hong Kong	Hong Kong
Ryan Wyatt	Other person involved in implementation	108 W. 13th Street, Suite 100, Wilmington, DE 19801	United States
Foris GFS Limited	Other person involved in implementation	Suite Nos. 5-7A, 17/F, Pacific Plaza, 410 Des Voeux Road W, Hong Kong 00000, Hong Kong	Hong Kong
Foris DAX, Inc.	Other person involved in implementation	c/o Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808, US	United States
James H. Grabow	Other person involved in implementation	110 N College Ave, Suite 500, Tyler, TX 75702	United States
Antonio Alvarez Lorenzo	Other person involved in implementation	110 N College Ave, Suite 500, Tyler, TX 75702	United States
Foris Holdings KY Limited	Other person involved in implementation	Could not be found	Cayman Islands

D.6 Utility Token Classification

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

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

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

D.8 Plans for the token

This section provides an overview of the historical developments related to the CRO crypto-asset and a description of planned or anticipated project milestones as publicly communicated. All forward-looking elements are subject to significant uncertainty. They do not constitute commitments, assurances or guarantees, and may be modified, delayed or discontinued at any time.

There is no single formally published roadmap for the CRO token; project plans and past developments are communicated through the project's website, its technical documentation, its blog, its official social media channels and on-chain governance proposals (sources: https://cronos.com/, https://cronos.com/about-cro, https://docs.cronos.com/, https://docs.cronos-pos.org/, https://blog.cronos.com/, https://www.mintscan.io/crypto-org/proposals, accessed 2026-08-06).

Past milestones:

- Project foundation (2016): the project was initially founded under the Monaco brand, with an early focus on crypto-based payment solutions and consumer-facing financial infrastructure. This entity later became the basis for the broader ecosystem within which the CRO crypto-asset was issued.

- Rebranding to Crypto.com (July 2018): Monaco was rebranded to Crypto.com, expanding its scope towards a global crypto platform encompassing payments, exchange services and supporting blockchain infrastructure.

- CRO supply reduction event (February 2021): a large-scale burn of 70,000,000,000 CRO was publicly announced as part of a supply restructuring communicated ahead of the launch of public blockchain infrastructure. The tokens were transferred to a publicly verifiable burn address and removed from circulation.

- Crypto.org Chain mainnet launch (March 2021): the Crypto.org Chain launched on mainnet as a Cosmos SDK based blockchain with CRO as its native asset, supporting payments, staking and governance. The chain was later renamed the Cronos POS Chain.

- Cronos EVM mainnet launch (November 2021): the Cronos EVM launched as an Ethereum Virtual Machine compatible Layer-1 network for smart contracts and decentralised applications.

- Cronos EVM exits beta (December 2022): the Galileo upgrade was announced as a major network milestone, introducing performance optimisations and expanded interoperability features, and positioning the Cronos EVM as a production network.

- Community pool burning mechanism (December 2023): proposal 18 was approved on the Cronos POS Chain, introducing a burning mechanism for the CRO community pool.

- Increase of the CRO inflation rate (February 2024): proposal 19 was approved on the Cronos POS Chain, increasing the CRO inflation rate from 0.06% to 10.00% per annum.

- Titan upgrade (March 2024): the Titan upgrade was implemented to increase node performance on the Cronos EVM.

- Cronos zkEVM alpha mainnet (December 2024): the Cronos zkEVM alpha mainnet was launched as a Layer-2 network secured via Ethereum, enabling early production use and supporting features such as account abstraction and yield-bearing representations of CRO. The network is being wound down, as described below.

- Re-minting of CRO and creation of a strategic reserve (March 2025): proposal #29 was approved on the Cronos POS Chain on 2025-03-16 and executed by a network upgrade on 2025-03-18, re-minting 70,000,000,000 CRO, corresponding to the amount burned in February 2021, and allocating it to a strategic reserve escrow address subject to linear vesting. The total supply of CRO was thereby restored to 100,000,000,000 units, while the tokens burned in 2021 remained out of circulation.

- Announcement of a CRO treasury vehicle (August 2025): a strategic arrangement was announced for the establishment of a publicly listed digital asset treasury vehicle holding CRO, to be formed through a business combination with a listed acquisition company. The transaction has not completed at the date of this white paper and remains subject to regulatory processes and other conditions.

- Launch of Cronos One (December 2025): Cronos One was launched as a unified onboarding interface consolidating cross-chain bridging, wallet top-up functionality and on-chain wallet verification. A component of it links a non-custodial wallet to a verified exchange account through a gasless process, publishing only a verifiable status rather than personal data. Cronos One was positioned as an identity and access layer for subsequent identity-aware and agent-driven applications.

- Cronos POS Chain v7 upgrade (May 2026): a network upgrade transitioned CRO from an emissions-based to a revenue-based staking model. It enforces a maximum supply of 100,000,000,000 CRO at protocol level, pins the inflation rate at 1.00% per annum subject to a monthly decay towards zero, and introduces time-locked staking positions earning bonus rewards above the base rate.

- Deprecation of the Cronos zkEVM (2026): the deprecation of the Cronos zkEVM Alpha Mainnet was announced, with development effort consolidated on the Cronos EVM.

- Repositioning of the project (2026): the project was repositioned as a settlement layer for stablecoins and tokenised assets, and the Cronos App was announced as its principal user-facing product.

- Cronos POS Chain v8 upgrade (July 2026): a further network upgrade was approved by on-chain governance and activated at block height 30,720,400, carrying maintenance changes including corrections to the time-locked staking module introduced by the v7 upgrade.

- Closed beta release of the Cronos App (July 2026): on 2026-07-27 the project announced that invitations to a closed beta of the Cronos App had been issued to a subset of users. The application is available by invitation only and is not generally available at the date of this white paper.

- Network halt and state restoration following an exploit of a third-party lending protocol (August 2026): on 2026-08-30 the project announced that it had identified an exploit in Tectonic, a lending protocol deployed on the network, and that the Cronos Network had been halted. The project described the halt as a validator-consensus emergency action. Block production was subsequently resumed and the project stated that the chain state had been restored to a point preceding the exploit, so that transactions recorded on the network between that point and the halt were reversed. The exploit was carried out by manipulating the price of a thinly traded token accepted as collateral by that protocol and borrowing against the inflated valuation; the protocol affected is not operated by the persons named in this white paper and the protocol of the crypto-asset itself was not the subject of the exploit. At the date of this white paper the project had stated that the network was under observation, that certain applications, service providers and bridging arrangements had not yet resumed normal operation, and that a full assessment of the incident had not yet been published (sources: https://x.com/CronosNetwork/status/2094072333434769703, https://x.com/CronosNetwork/status/2094417832394301499, accessed 2026-08-31).

Future milestones:

- General availability of the Cronos App (2026): the project has announced the Cronos App, a self-custody application for trading, and operates a waitlist for access. The application has not been made generally available at the date of this white paper. The project states that availability is subject to jurisdictional limitations and that the features described do not constitute a commitment to deliver any material, code or functionality.

- Desktop version of the Cronos App (2026): a desktop version of the Cronos App has been announced and is described by the project as forthcoming.

- Application of ecosystem revenue to the rewards pool: infrastructure to channel protocol revenue from the wider Cronos ecosystem, including the Cronos App, to the Cronos POS Chain rewards pool was delivered by the v7 upgrade. The project has stated an intention that this revenue progressively fund the bonus rewards on time-locked staking positions as issuance decays. The Cronos App is not generally available at the date of this white paper and no revenue from it is being applied in this way.

- Release of the strategic reserve: the project has stated that the remaining undeployed portion of the strategic reserve is governed by a multi-year release schedule intended to support staking rewards, developer growth, network security and ecosystem expansion.

- Decommissioning of the Cronos zkEVM (from 2027-06-03): following the bridging deadline of 2027-06-03, the Cronos zkEVM is to be fully decommissioned.

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

D.9 Resource allocation

According to publicly available information (sources: https://blog.cronos.com/, https://crypto.com/company-news, https://docs.cronos-pos.org/, accessed 2026-08-06), the development of the wider group within which the crypto-asset originated was initially funded by a token sale conducted between 2017-05-18 and 2017-06-18, which raised approximately USD 26,700,000 through the sale of a predecessor token. The project's own 2018 publication states that the CRO crypto-asset itself was distributed by secondary distribution only, with no pre-sale, no public sale and no initial coin offering, so no proceeds were raised through the issuance of CRO. In July 2026 a strategic investment of USD 400,000,000 by an institutional investor was announced at a stated valuation of USD 20,000,000,000, described as the first institutional funding round in the group's history and stated to be intended to accelerate expansion into further asset classes, including tokenised securities and derivatives. The announcement does not identify the legal entity receiving the investment and does not state the resulting shareholding.

The project's 2018 publication set out the allocation of the total supply of 100,000,000,000 CRO across five categories, held in separate multi-signature addresses: 30,000,000,000 for secondary distribution and launch incentives, released on a tapering five-year schedule; 20,000,000,000 for network long-term incentives; 20,000,000,000 as a capital reserve; 20,000,000,000 for ecosystem grants; and 10,000,000,000 for an airdrop to holders of the predecessor token and for community development. That allocation was subsequently affected by the burn of 70,000,000,000 CRO in February 2021 and by the re-minting of the same number of tokens in March 2025, the re-minted tokens being allocated to a strategic reserve escrow address subject to linear vesting. The project states that the undeployed portion of that reserve is governed by a multi-year release schedule intended to support staking rewards, developer growth, network security and ecosystem expansion.

No allocation of the funding described above to the crypto-asset project specifically has been disclosed, and the extent to which the resources of the wider group are attributable to the crypto-asset project cannot be determined from publicly available sources. This limits the ability to assess the funding and staffing dedicated specifically to this project.

The token distribution can be traced on-chain on the Cronos POS Chain: https://cronos-pos.org/explorer#balances. The investor must be aware that a public address cannot necessarily be

assigned to a single person or entity, which limits the ability to determine exact economic influence or future actions.

However, all such information is derived exclusively from the project's own publications, public announcements, governance records and third-party publications. The issuer, foundation, or entities associated with the CRO crypto-asset have not independently confirmed the occurrence, precise amounts, valuation, legal structure, or contractual terms of these reported financing rounds and allocations. As a result, the referenced investment amounts, allocation figures and any implied cumulative funding figures cannot be independently verified and should be considered indicative only. Token distribution changes can negatively impact the investor.

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

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The maximum supply of the crypto-asset is 100,000,000,000 units. Following a network upgrade activated on the Cronos POS Chain in May 2026, this maximum is enforced at protocol level and no units may be issued in excess of it. New units continue to be issued as validator rewards, at an inflation rate pinned at 1.00% per annum and subject to a monthly compound decay towards zero, so the total supply may increase over time but cannot exceed the maximum. The parameters governing the maximum supply and the issuance of new units remain adjustable by on-chain governance. Investors should note that changes in the token supply can have a negative impact. The effective amount of tokens available on the market depends on the number of tokens released by the issuer or other parties at any given time, as well as potential reductions through token 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 transaction fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

F.2 Crypto-asset functionality

According to publicly available information (sources: https://cronos.com/about-cro, https://docs.cronos.com/, https://docs.cronos.com/cronos-chain-protocol/cronos-general-faq, https://docs.cronos-pos.org/, accessed 2026-08-06), CRO is the native crypto-asset of the Cronos ecosystem, which comprises the Cronos POS Chain and the Cronos EVM. CRO exists natively within the Cronos infrastructure and is also issued in bridged form on other blockchain networks for compatibility and liquidity purposes.

1. Transaction execution and fee settlement:

CRO functions as the native transaction fee (gas) asset across the Cronos ecosystem. On the Cronos POS Chain, CRO is used to pay transaction fees associated with base-layer operations secured by proof-of-stake consensus. On the Cronos EVM, CRO is likewise used to pay gas fees for smart-contract execution and transaction processing within the Ethereum-compatible environment. Transaction fees are dynamically calculated and collected by validators according to protocol rules and network conditions.

A third network, the Cronos zkEVM, used a derivative asset rather than CRO to pay transaction fees. That network is being wound down and holders of assets on it have been directed to transfer them off it by 2027-06-03, after which access to those assets may be limited. CRO is not, and was not, the fee asset on that network.

2. Network security, staking, and reward distribution:

Within the Cronos POS Chain, CRO is the asset through which economic participation in network security is facilitated. Validators and delegators participate in the proof-of-stake process by bonding CRO, thereby contributing to block production, transaction validation and finality, and receive protocol-level rewards in return.

The Cronos EVM operates on a proof-of-authority consensus mechanism derived from Tendermint proof-of-stake consensus, under which the validator set is permissioned and validator hosting is by invitation only. CRO is not used for validator staking or governance on that network, and its role there is limited to the payment of transaction fees and application-level utility.

Following a network upgrade activated in May 2026, rewards may be earned at a base rate on flexible bonded positions, or at higher rates on positions locked for a fixed term. Three lock terms are available, of one, two and four years, earning additional rates of 2.00%, 4.00% and 7.00% respectively above the base rate. Voting rights, redelegation between validators and withdrawal of accrued rewards are preserved during a lock. Reward rates are variable and are determined by protocol parameters that may be changed by on-chain governance. The same upgrade changed the funding of these rewards. Newly issued CRO continues to be distributed as block rewards, at an inflation rate pinned at 1.00% per annum and subject to a monthly compound decay towards zero, within an enforced maximum supply of 100,000,000,000 units. As issuance declines, the project states that rewards are funded from a strategic reserve of CRO and are intended over time to be funded from revenue generated within the ecosystem, including by the Cronos App. The Cronos App is not generally available at the date of this white paper. Whether, when and to what extent such revenue arises is uncertain, and no assurance is given that rewards will be maintained at any particular rate.

3. Governance-related coordination:

Governance participation using CRO is limited to protocol-level decision-making on the Cronos POS Chain, where holders who bond or delegate their CRO may participate in governance processes such as parameter changes and network upgrades, subject to validator mediation. Governance rights relate exclusively to technical and protocol-level matters and do not extend to decision-

making authority over any legal entity associated with the Cronos ecosystem or its contributors. Matters determined by that process include the parameters governing issuance and the maximum supply. CRO does not confer governance rights on the Cronos EVM beyond that network's protocol rules.

4. Ecosystem and application-level utility:

CRO serves as a medium of exchange and liquidity asset within decentralised applications deployed across the Cronos ecosystem, including decentralised finance protocols, NFT marketplaces and liquidity pools. It is commonly used as a base asset for trading pairs, incentive mechanisms and collateral configurations, depending on the design of individual applications. Beyond on-chain usage, CRO is integrated into centralised products, including payment services, reward programmes and card-based incentive structures. These uses are application-level and contractual in nature and are distinct from CRO's protocol-level functions within the Cronos blockchains. A portion of CRO is also removed from circulation by transfer to a publicly verifiable burn address, from which it cannot be recovered. The project states that revenue generated within the ecosystem is intended to be applied in part to purchases of CRO and to such transfers.

The CRO crypto-asset does not confer ownership, profit participation, or claim rights over the Cronos protocol or any affiliated foundation or operating entity. All functionalities of CRO are technical and operational, relating exclusively to transaction processing, network security incentives, governance coordination and application-level interactions within the Cronos ecosystem. The actual usability of CRO depends on factors such as network stability, validator participation, smart-contract execution, protocol upgrades, interoperability mechanisms and broader market conditions, all of which are outside the control of individual holders.

F.3 Planned application of functionalities

Future milestones:

- General availability of the Cronos App (2026): the project has announced the Cronos App, a self-custody application for trading, and operates a waitlist for access. The application has not been made generally available at the date of this white paper. The project states that availability is subject to jurisdictional limitations and that the features described do not constitute a commitment to deliver any material, code or functionality.

- Desktop version of the Cronos App (2026): a desktop version of the Cronos App has been announced and is described by the project as forthcoming.

- Application of ecosystem revenue to the rewards pool: infrastructure to channel protocol revenue from the wider Cronos ecosystem, including the Cronos App, to the Cronos POS Chain rewards pool was delivered by the v7 upgrade. The project has stated an intention that this revenue progressively fund the bonus rewards on time-locked staking positions as issuance decays. The Cronos App is not generally available at the date of this white paper and no revenue from it is being applied in this way.

- Release of the strategic reserve: the project has stated that the remaining undeployed portion of the strategic reserve is governed by a multi-year release schedule intended to support staking rewards, developer growth, network security and ecosystem expansion.

- Decommissioning of the Cronos zkEVM (from 2027-06-03): following the bridging deadline of 2027-06-03, the Cronos zkEVM is to be fully decommissioned.

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

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

The type of submission is MODI, which stands for "Modification".

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than an e-money token (EMT) or an asset-referenced token (ART). It is issued natively on the Cronos POS Chain and on the Cronos EVM, and is additionally available in bridged form on other distributed-ledger networks. The crypto-asset is fungible. It is divisible to 8 decimal places on the Cronos POS Chain and in its representations on other networks, and to 18 decimal places as the native asset of the Cronos EVM. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, legally enforceable governance rights, profit participation, or any other legally enforceable rights. Any functionalities associated with the crypto-asset are limited to technical features within the relevant network 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. 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: "Cronos" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-08-06).

F.8 Website of the issuer

https://crypto.com/

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

2026-02-18

F.10 Publication date

2026-02-18

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

DQG22RKCR; W4DBTJQ98; ZBC8DTX8G; G0V71VTTX; 2MPCC77C1; 5VNCFR2T5; C77WR20TB; D00BX2H21

F.14 Functionally fungible group digital token identifier

GWM30MLW3

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are of a

purely technical or operational nature and do not constitute rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments. Accordingly, holders do not acquire any legally enforceable claim against the issuer of the crypto-asset or any third party.

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on the future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-08-05).

G.5 Issuer retained crypto-assets

Based on publicly available on-chain data, 62,116,666,648 CRO, being approximately 62% of the total supply of 100,000,000,000 CRO, are currently held in the Cronos Strategic Reserve escrow address and its directly identified collection address. A further approximately 6,800,000,000 CRO released from the Strategic Reserve cannot be located in the available public transaction history. The project states that approximately 95% of vested CRO remains held in reserve, which would imply a reserve-associated total of approximately 69,000,000,000 CRO, or around 69% of the total supply. That statement is consistent with the movements that can be observed but cannot be independently verified.

In March 2025, 70,000,000,000 CRO were issued to the Cronos Strategic Reserve as part of the Cronos POS V5 upgrade and placed under a five-year monthly vesting schedule ending in March 2030. Of that allocation, 51,333,333,333 CRO remain unvested in the escrow address.

The exact number of CRO retained by the issuer itself has not been confirmed by the issuer. Public blockchain data does not independently establish the beneficial ownership or control of all relevant addresses, and the allocation or ownership of CRO may change over time. Accordingly, the figures above should be understood as an estimate based on publicly available information rather than as a confirmed statement of the issuer's holdings.

G.6 Utility token classification

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

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

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

G.8 Utility tokens redemption

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

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-08-06.

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

G.13 Supply adjustment mechanisms

Not applicable.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DLT)

The crypto-asset in scope is implemented on the Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Osmosis and Solana networks following the standards described below.

H.2 Protocols and technical standards

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Solana and Osmosis. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Cronos PoS Chain:

1. Network protocols. Cronos POS Chain is built using the Cosmos SDK and uses CometBFT, the successor to Tendermint Core, for its Proof-of-Stake Byzantine Fault Tolerant consensus. Validators participate in block production and consensus, while non-validating full nodes maintain and serve blockchain data.

2. Transaction and address standards. Accounts use Bech32 addresses with the mainnet prefix cro. Standard secp256k1 account addresses are derived by applying SHA-256 and RIPEMD-160 to the public key and encoding the resulting 20-byte identifier in Bech32 format. Transactions specify a gas limit and fee amount, the ratio of which represents the effective gas price.

3. Blockchain data structure and block standards. Application state is managed through modular Cosmos SDK state machines, while CometBFT provides block and consensus structures. Blocks contain transaction data and consensus information, with cryptographic commitments in the block header including the application state commitment (AppHash). Once committed through CometBFT consensus, blocks achieve deterministic finality.

4. Interoperability protocols. Cronos POS Chain supports the Inter-Blockchain Communication (IBC) protocol for cross-chain communication and token transfers with compatible IBC-enabled networks.

5. Upgrade and improvement standards. Network changes and software upgrades may be approved through on-chain governance and implemented through updated node software. Governance voting power is based on eligible staked CRO; delegators generally inherit the vote of their validator unless they vote independently.

The following applies to Cronos EVM Chain:

1. Network Protocols

Cronos EVM Chain is a public, EVM-compatible Layer-1 built with the Cosmos SDK and Ethermint (porting go-ethereum/EVM execution to Cosmos). Consensus runs on CometBFT (Tendermint-class BFT); the consensus mechanism is described in section H4. The protocol is open-source and maintained in public repositories.

2. Transaction and Address Standards

Accounts use 20-byte 0x-prefixed EVM addresses (Keccak-derived). Transactions consume gas (gas used × gas price) paid in CRO and follow standard Ethereum formats supported by Ethermint: legacy (type-0), access-list (type-1), dynamic-fee (type-2) and, since the Smarturn upgrade of 30 October 2025, set-code (type-4, EIP-7702).

3. Blockchain Data Structure & Block Standards

State is managed via Cosmos SDK modules with EVM execution by Ethermint. Each block contains proposer/validator commits, transactions, and state commitments. Accounts and contract storage follow the Ethereum account model, but state is committed through the Cosmos SDK store rather than an Ethereum state trie. Effective block capacity is bounded by gas limits and consensus parameters rather than a fixed byte size.

4. Interoperability Protocols

Cronos EVM Chain is designed for Ethereum-tooling compatibility (Solidity/Vyper, JSON-RPC) and for inter-chain connectivity within the Cosmos stack via IBC where channels are established. Third-party bridges may provide additional connectivity, each with its own trust and operational assumptions.

5. Upgrade & Improvement Standards

Upgrades and parameter changes are governed on-chain via Cosmos SDK governance (proposal, voting, coordinated releases). The client software and EVM compatibility evolve through scheduled open-source releases; operators are expected to maintain version parity with governance decisions.

The following applies to Ethereum:

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

1. Network protocols

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

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

2. Transaction and address standards

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

The protocol currently supports the following transaction types:

- Type 0: legacy transactions (pre-EIP-1559).

- Type 1: access-list transactions (EIP-2930).

- Type 2: dynamic-fee transactions with base-fee burning (EIP-1559).

- Type 3: blob-carrying transactions (EIP-4844), introduced with the Dencun upgrade on 2024-03-13.

- Type 4: set-code transactions (EIP-7702), introduced with the Pectra upgrade on 2025-05-07, allow externally owned accounts (EOAs) to authorise delegated code execution during transactions, without permanently converting the account into a smart contract. This enables features such as transaction batching, sponsored gas payments and delegated signing.

3. Blockchain data structure and block standards

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

Each block contains:

- a block header, comprising the parent hash, state root, transactions root, receipts root, timestamp, gas limit and gas used, among other fields;

- the ordered list of transactions, including smart-contract executions and value transfers; and

- blob commitments, where applicable, referring to data published to the data availability layer under EIP-4844.

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

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

4. Upgrade and improvement standards

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

The following applies to Cosmos (ATOM):

1. Network Protocols

The Cosmos ecosystem operates on a modular and decentralised architecture designed to ensure deterministic consensus and interoperability. Consensus and peer-to-peer networking are provided by CometBFT (formerly Tendermint Core), which implements a Byzantine Fault Tolerant Proof-of-Stake consensus mechanism under which validators propose and vote on blocks to achieve finality. Communication between the consensus layer and the application layer is handled through the Application BlockChain Interface (ABCI). Cross-chain interoperability is enabled through the Inter-Blockchain Communication (IBC) protocol, which allows independent blockchains to exchange messages and transfer crypto-assets using cryptographic proofs.

2. Transaction and Address Standards

Transactions are defined at the application level and validated through a standardised processing pipeline that includes signature verification, nonce checks, gas accounting, and fee deduction.

Accounts store authentication information such as public keys, addresses, and sequence numbers, with addresses commonly represented using Bech32 encoding. Standard transaction types support asset transfers, staking, and governance actions, while IBC introduces packet-based transactions that enable verified cross-chain communication. Transaction fees are determined by chain-specific fee markets and are typically paid using the network's native staking crypto-asset.

3. Blockchain Data Structure & Block Standards

The blockchain architecture separates consensus from state execution, with CometBFT responsible for block ordering and the application layer responsible for deterministic state transitions. Application state is maintained using Merkle-based data structures, including Simple Merkle Trees and IAVL+ trees, producing a cryptographic state root (AppHash) that is committed to each block header via the ABCI Commit process and signed by a supermajority of validators.

4. Upgrade & Improvement Standards

Protocol changes and network upgrades are coordinated through on-chain governance and scheduled upgrade mechanisms that activate protocol changes at predefined block heights. Validators are required to run updated software at the scheduled upgrade point, enabling coordinated upgrades without unsynchronised network halts.

The following applies to Solana:

The crypto-asset is implemented on the Solana blockchain, a decentralised distributed-ledger network designed to support transaction processing and the execution of on-chain programs. The network relies on a set of technical protocols, cryptographic standards, and program frameworks intended to enable secure transaction validation, deterministic execution of instructions, and interoperability across the Solana ecosystem. The most relevant technical standards and protocols are outlined below.

1. Network Architecture and Core Protocols

The Solana network is structured as a peer-to-peer validator network in which independent nodes maintain the distributed ledger and process transactions.

- Solana uses Proof-of-History (PoH) as a cryptographic timing and ordering mechanism, while validator participation and voting are stake-weighted under its Proof-of-Stake model and Tower BFT consensus process.

- Tower BFT: A Byzantine fault tolerant consensus mechanism, derived from PBFT, that governs validator voting and block confirmation.

- Turbine: A block propagation protocol that distributes blocks across the validator network by splitting them into smaller data fragments ("shreds") and transmitting them through a layered tree-based structure.

- Gulf Stream: A transaction forwarding mechanism that routes transactions directly to upcoming block producers and thereby limits the need for a global transaction mempool.

- Sealevel: A parallel transaction execution engine that enables non-conflicting transactions and programs to execute simultaneously across multiple processing threads.

Together, these mechanisms support transaction processing while maintaining a synchronised and verifiable ledger state across participating validator nodes.

2. Address and Cryptographic Standards

Accounts and transactions on the Solana network rely on defined cryptographic primitives and address formats.

- Account Addresses: Accounts are identified by 32-byte addresses. Externally controlled accounts typically use Ed25519 key pairs, while program-derived addresses (PDAs) are deterministically derived off-curve addresses that do not correspond to a private key.

- Transaction Signatures: Transactions are authorised through Ed25519 signatures associated with the account owner's keypair.

- Hashing: Sequential SHA-256 hashing is used within the Proof-of-History mechanism to generate a verifiable ordering of events.

- Program Derived Addresses (PDAs): Deterministically generated addresses derived through hashing procedures that ensure the resulting address does not correspond to a private key, thereby enabling secure program-controlled accounts.

These cryptographic mechanisms provide the basis for transaction authentication, deterministic account control, and verifiable execution of on-chain instructions.

3. Networking and Data Transmission Standards

Communication between validator nodes and network participants follows defined networking protocols and technical constraints.

- QUIC is used for transaction ingress and TPU-related forwarding paths on Solana validators, alongside other networking channels used across the cluster.

- UDP-based propagation: Utilised for distributing block fragments ("shreds") across the network through the Turbine protocol.

- Transaction size limits: The maximum transaction size of approximately 1,232 bytes is aligned with the IPv6 minimum transmission unit (MTU) after accounting for network headers, and is intended to enable atomic transmission without fragmentation.

- JSON-RPC interfaces: Standardised APIs used by wallets, applications, and infrastructure providers to submit transactions and query blockchain state.

These standards support interoperability between network nodes, developer infrastructure, and user-facing applications interacting with the Solana ledger.

4. Token and Program Standards (Solana Program Library)

Tokens on Solana are commonly implemented using either the original Token Program or the Token Extension Program (Token-2022), each of which defines standardised token behaviour through on-chain program logic.

Within this framework:

- A token type is represented by a mint account, which defines parameters such as total supply and mint authority.

- Individual token balances are stored in token accounts, which hold balances associated with a specific mint and owner address.

- Interactions with tokens occur through instructions executed by the relevant token program rather than through separate token-specific smart contracts.

These programmatic standards enable consistent token management across the Solana ecosystem. Projects may also integrate metadata functionality, for example through the Metaplex Token Metadata Program or, where applicable, through Token-2022 metadata extensions.

5. Protocol Development and Improvement Standards

Technical changes to the Solana protocol may be proposed and discussed through Solana Improvement Documents (SIMDs). These proposals document suggested modifications to protocol behaviour, economic parameters, or technical limits. Accepted changes may be implemented through updates to validator software and related developer tooling used by network participants.

The following applies to Osmosis:

1. Network Protocols

Osmosis is an application-specific Layer 1 blockchain built using the Cosmos SDK. Consensus and peer-to-peer networking are provided through CometBFT, formerly Tendermint Core, which

implements Byzantine Fault Tolerant state-machine replication. Osmosis also supports cross-chain communication through the Inter-Blockchain Communication protocol, which enables transfers and messages between IBC-enabled chains.

2. Transaction and Address Standards

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

3. Blockchain Data Structure & Block Standards

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

4. Upgrade & Improvement Standards

Protocol upgrades are coordinated through Osmosis governance and scheduled software upgrades. Validators are required to run compatible software at the relevant upgrade point. As an IBC-connected chain, Osmosis upgrades must also preserve compatibility with IBC clients, channels, and counterparty chains where applicable.

H.3 Technology used

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Solana and Osmosis. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Cronos PoS Chain:

1. Decentralised ledger. Cronos POS Chain is a public blockchain built on the Cosmos SDK and using CometBFT for Proof-of-Stake Byzantine Fault Tolerant consensus. Transactions and resulting state changes are recorded on a publicly verifiable ledger, and blocks achieve deterministic finality once committed under the applicable consensus assumptions.

2. Private key management. CRO may be managed through compatible software and hardware wallets. Accounts use Bech32 addresses, generally with the cro prefix for account addresses. For self-custodied holdings, users are responsible for safeguarding their private keys and recovery material; loss of all means of recovering the relevant keys may result in permanent loss of access to the associated CRO.

3. Cryptographic integrity. Cronos POS Chain uses public-key cryptography for transaction authentication and validator consensus. The network supports secp256k1 and secp256r1 keys for transaction signing, while validator consensus signatures use Ed25519 keys. Cryptographic signatures and hashes enable verification of transactions, blocks and blockchain state.

4. Network security. Validator participation is permissionless in the sense that any party may create a validator by providing a self-delegation; the active validator set consists of the 100 validators with the highest bonded stake. Validators specify a minimum self-delegation and are subject to protocol penalties for specified consensus or liveness failures. Under the CometBFT security model, consensus safety is maintained provided that less than one-third of total voting power acts Byzantine.

The following applies to Cronos EVM Chain:

1. Decentralised Ledger

Transactions in CRO are recorded on a transparent, append-only ledger. Blocks are finalised upon commit, subject to network parameters and validator participation. Execution is optimised for throughput through concurrent transaction processing within each block (Block-STM) and the MemIAVL storage layer.

2. Private Key Management

Users interact via EVM-compatible wallets (for example MetaMask, Ledger, Crypto.com Onchain). Accounts follow the Ethereum model with 0x-prefixed, 20-byte addresses derived from public keys (Keccak-256). Users are responsible for safeguarding private keys and recovery phrases; the network does not custody user keys.

3. Cryptographic Integrity

End-user transactions are signed using ECDSA over secp256k1 (Ethereum signature scheme). Validator consensus keys follow CometBFT conventions (ed25519 for commits). Execution follows the EVM account and storage model, with state committed and verified through the Cosmos SDK store.

The following applies to Ethereum:

1. Decentralised Ledger: The Ethereum blockchain acts as the decentralised ledger and execution environment for ETH transactions and smart-contract operations, including ERC-20 token transfers, maintaining an append-only record of transfers and account balances to support transparency and verifiable settlement.

2. Account Model: Ethereum uses two account types: externally owned accounts (EOAs), which are controlled through private keys, and contract accounts, which are controlled through deployed smart contract code. Following the Pectra upgrade on 2025-05-07, EOAs can additionally authorise

delegated code execution through EIP-7702 transactions without permanently converting the account into smart contracts.

3. Private Key Management: Users must securely store the private keys and recovery material associated with their wallets. Loss or compromise of a private key may result in irreversible loss of access to the associated ETH or ERC-20 token balance.

4. Cryptographic Integrity: Ethereum uses ECDSA over the secp256k1 elliptic curve for key generation and digital signatures on the execution layer. Keccak-256 hashing is used for transaction hashing, state hashing and address derivation. Ethereum addresses are derived from the last 20 bytes of the Keccak-256 hash of the public key. On the consensus layer, BLS (Boneh-Lynn-Shacham) signatures are used to aggregate validator attestations under the Proof-of-Stake consensus mechanism.

The following applies to Cosmos (ATOM):

1. Decentralised Ledger

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

2. Private Key Management

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

3. Modular Design and Smart Contracting

The Cosmos Hub follows a modular architecture based on the Cosmos SDK. While the Hub itself focuses on native asset transfers and staking, smart-contract functionality may be provided through CosmWasm-based modules or connected application chains, where token logic and application-level rules are implemented outside the core ledger.

The following applies to Solana:

1. Solana-Compatible Wallets: The tokens are generally supported by wallets compatible with Solana's token programs.

2. Decentralised Ledger: The Solana blockchain acts as a decentralised ledger for all token transactions, with the intention of preserving a tamper-resistant record of token transfers and ownership in order to ensure both transparency and security.

3. SPL Token Program: Tokens on Solana are commonly implemented using either the original Token Program or the Token Extension Program (Token-2022), which provide standardised on-chain logic for token creation, issuance, transfer, and account management. Unlike the ERC-20 model on Ethereum, where a project typically deploys its own token contract, Solana tokens generally rely on shared token-program infrastructure, which promotes a high degree of standardisation across the ecosystem.

4. Blockchain Scalability: Solana is designed to support high transaction throughput and comparatively low transaction fees, with the intention of enabling efficient token transfers and related on-chain operations.

Security Protocols for Asset Custody and Transactions:

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

2. Cryptographic Integrity: Solana uses Ed25519 digital signatures to authenticate transactions submitted by authorised signers, thereby supporting the integrity and verifiability of token transfers.

The following applies to Osmosis:

1. Decentralised Ledger

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

2. Private Key Management

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

3. Modular Design and Smart Contracting

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

H.4 Consensus mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Solana and Osmosis. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Cronos POS:

Cronos POS Chain uses the CometBFT Proof-of-Stake consensus mechanism, based on the Tendermint BFT consensus protocol. Voting power is proportional to bonded CRO, comprising the validator's self-bonded stake and CRO delegated to it by holders. For each consensus round, a proposer is selected according to voting power and proposes a candidate block. Validators then proceed through the proposal, prevote and precommit stages. A block is committed and achieves deterministic finality once more than two-thirds of total voting power has precommitted to it, subject to the applicable Byzantine Fault Tolerance assumptions. Full nodes relay transactions and maintain and serve blockchain data but do not participate in block production unless they operate as active validators.

The following applies to Cronos EVM Chain:

Cronos EVM Chain secures its network with CometBFT (Tendermint-class) Byzantine Fault Tolerant consensus and a permissioned validator set, commonly described as a PoA-style variant of Proof-of-Stake. Designated validators propose and commit blocks in BFT rounds, and validator admission is by invitation under network governance. Safety holds provided fewer than one third of voting power is faulty or malicious. Blocks are final on commit, so there is no probabilistic confirmation period. Misbehaviour or insufficient liveness is penalised under protocol rules, including slashing for double-signing and jailing or tombstoning under the consensus parameters. Validators are expected to operate with high-availability infrastructure, redundancy, and standard network protections (for example DDoS mitigation). Finality on commit is a property of the consensus protocol and not a guarantee that the recorded state will be preserved. Where a sufficient share of voting power agrees to do so, the validator set is able to suspend block production and to resume it from an earlier state, with the effect that transactions previously committed and treated as final are reversed. This occurred on the network in August 2026.

The following applies to Ethereum:

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

The following applies to Cosmos (ATOM):

The Cosmos Hub operates a Proof-of-Stake (PoS) consensus mechanism based on CometBFT (formerly Tendermint consensus), a Byzantine Fault Tolerant (BFT) algorithm designed to provide fast finality and deterministic state replication.

Consensus participants are validators who bond the native crypto-asset ATOM as collateral and obtain voting power proportional to their bonded stake, including delegated ATOM from third parties. Validators participate in block production and consensus by proposing blocks and broadcasting cryptographic votes.

Consensus proceeds in rounds, each consisting of a block proposal, followed by two voting phases (pre-vote and pre-commit). A block is finalised and irreversibly committed once more than two-thirds of the total validator voting power pre-commits to the same block in the same round. This mechanism provides immediate finality and prevents probabilistic forks.

CometBFT ensures Byzantine Fault Tolerance, meaning the network remains safe and consistent as long as less than one-third of total voting power behaves maliciously or fails. The Cosmos Hub maintains a bounded validator set, initially capped at 100 validators and designed to increase gradually over time to balance decentralisation and performance.

The following applies to Solana:

Solana uses a combination of Proof-of-History (PoH) and Proof-of-Stake (PoS). The core concepts of the mechanism are intended to work as follows:

Core Concepts

1. Proof-of-History (PoH):

PoH is a cryptographic ordering and timing mechanism that provides evidence that data existed in a particular sequence and that time passed between proofs.

Verifiable Delay Function (VDF): PoH relies on a sequential hash-based proof process that Solana describes as VDF-like. This sequence of hashes provides a verifiable order of events, enabling the network to efficiently agree on the sequence of transactions.

2. Proof-of-Stake (PoS):

Validator Selection: Leader slots are assigned through the network's leader schedule, which is stake-weighted. The more SOL staked, the higher the chance of being selected to validate transactions and produce new blocks.

Delegation: Token holders can delegate their SOL tokens to validators, earning rewards proportional to their stake while contributing to the network's security.

Consensus Process

1. Transaction Validation:

Transactions are broadcasted to the network and collected by validators. Each transaction is validated to ensure it meets the network's criteria, such as having correct signatures and sufficient funds.

2. PoH Sequence Generation:

A validator generates a sequence of hashes using PoH, each containing a timestamp and the previous hash. This process creates a historical record of transactions, establishing a cryptographic clock for the network.

3. Block Production:

The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order.

4. Consensus and Finalisation:

Other validators vote on the ledger state associated with the block. A block may first become confirmed and later finalised once it reaches the network's strongest confirmation state.

Security and Economic Incentives

1. Incentives for Validators:

Block Rewards: Validators earn rewards for producing and validating blocks. These rewards are distributed in SOL tokens and are proportional to the validator's stake and performance.

Transaction Fees: Validators also earn transaction fees from the transactions included in the blocks they produce. These fees provide an additional incentive for validators to process transactions efficiently.

2. Security:

Staking: Staking provides economic alignment, and Solana documentation notes that slashing has been discussed as a future mechanism for intentional malicious behaviour, but is not implemented yet.

Delegated Staking: Token holders can delegate their SOL tokens to validators, intended to enhance network security and decentralisation. Delegators share in the rewards and are incentivised to choose reliable validators.

3. Economic Penalties:

Slashing (planned): Validators can be penalised for malicious behaviour, such as double-signing or producing invalid blocks. This penalty, known as slashing, results in the loss of a portion of the staked tokens, discouraging dishonest actions.

The following applies to Osmosis:

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

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

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

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

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

H.5 Incentive mechanisms and applicable fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Solana and Osmosis. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Cronos PoS Chain:

Cronos POS incentivises validators and delegators through staking rewards. Validators receive rewards based on bonded CRO, while CRO holders may delegate to validators and receive a share of the rewards after deduction of the validator's commission. Rewards comprise newly issued CRO and transaction fees; following the 2026 tokenomics upgrade, CRO emissions follow a governance-adjustable decay mechanism, while additional staking rewards may be funded from the dedicated rewards pool. Optional time-locked staking tiers provide additional rewards for longer-term commitments.

Validators are subject to penalties for consensus faults and insufficient liveness. Double-signing may result in slashing and permanent removal from validator participation, while extended downtime may result in slashing and temporary jailing. Delegated CRO is exposed to the same applicable slashing risk as the validator's stake.

The following applies to Cronos EVM Chain:

Validators on the Cronos EVM are remunerated from transaction fees paid in CRO. The validator set is permissioned and admission to it is by invitation, and CRO is not used for validator staking or for governance on that network. Fees are gas-based, being gas used multiplied by gas price, and are paid in CRO. A base fee is set for each block by the fee market module and adjusts upwards or downwards with network usage measured against a gas target. Fee parameters, including the base fee and the minimum gas price, are chain parameters and may be changed by governance.

The following applies to Ethereum:

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

The following applies to Cosmos (ATOM):

The Cosmos Hub secures its Proof-of-Stake consensus mechanism through an integrated system of economic incentives and penalties. This framework is designed to encourage honest participation by validators and delegators, deter malicious or negligent behaviour, and ensure the long-term security and sustainability of the network.

Incentive Mechanisms (Rewards)

Validators and delegators are rewarded for participating in block production and consensus through a combination of inflationary issuance and transaction fees. The native staking crypto-asset ATOM is issued as an inflationary reward and distributed to bonded validators and delegators in proportion to their bonded stake. In addition, users pay transaction fees, which are collected by validators and periodically redistributed to bonded participants, subject to validator-defined commission rates.

Transaction Fees

The Cosmos Hub applies a gas-based fee model to limit network spam and compensate network operators. Fees are calculated based on transaction complexity and size using a gas limit and a gas price, and are deducted from the transaction signer prior to execution. Validators may set their own minimum gas prices and may accept multiple token denominations as fees, selecting which transactions to include within block gas limits.

Fee Distribution and Reserve Pool

Collected transaction fees are redistributed at regular intervals to bonded validators and delegators in proportion to their bonded ATOM. A predefined portion of these fees (by default 2%) is allocated to a reserve pool, which is intended to support network security and sustainability and may be distributed through on-chain governance decisions.

Penalties and Slashing

Bonded ATOM functions as economic collateral and is subject to slashing in the event of protocol violations. Validators that commit safety faults, such as double-signing conflicting blocks at the same height, are subject to significant slashing and are typically permanently removed from the validator set.

The following applies to Solana:

1. Validators:

Validators participate in block production and voting under Solana’s stake-weighted model. They may receive staking-related rewards and a share of transaction-fee income. Under Solana’s fee model, the base fee is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This is intended to provide an additional financial incentive for validators to process transactions efficiently and maintain the network's integrity.

2. Delegators:

Delegated Staking: Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share the rewards earned by the validators. This is intended to encourage widespread participation in securing the network and to support decentralisation.

3. Economic Security:

Solana staking documentation notes slashing as a possible future mechanism for intentional malicious conduct, but states that slashing is not implemented in the protocol today. Economic alignment instead currently arises primarily from staking participation, validator performance incentives, and the opportunity cost of locking capital in staking positions.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana transactions require fees in SOL. The fee model consists of a base fee and, where used, an optional prioritisation fee. The base fee compensates signature verification work and is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

2. Rent Fees:

Solana accounts that store on-chain state must satisfy the rent-exemption threshold, which is linked to the amount of data stored. This mechanism is intended to support efficient use of network state and account storage resources.

3. Program Execution Costs:

Deploying and interacting with on-chain programs may involve transaction fees and, where relevant, compute-related prioritisation fees and account-storage requirements. These mechanisms are intended to allocate network resources in proportion to use.

The following applies to Osmosis:

1. Validator and Delegator Rewards

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

2. Liquidity Provider Incentives

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

3. Transaction Fees

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

4. Slashing and Penalties

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

H.6 Use of distributed ledger technology

Yes – DLT operated by the issuer or a third-party acting on the issuer's behalf.

H.7 DLT functionality description

The crypto-asset is transferred and stored on two networks operated on different bases.

On the Cronos EVM, block production is carried out by a permissioned validator set operating a proof-of-authority consensus mechanism. Admission to that set is by invitation, applications are not open, and candidates are selected against security and performance criteria including background checks. The published route for registering an interest in becoming a validator is an address maintained by an entity connected to the crypto-asset project and named in this white paper as a person involved in its implementation. Participation in block production on that network is therefore not open to any person on equal terms, and the composition of the set that produces blocks is determined by persons connected to the project (source: https://docs.cronos.com/cronos-chain-protocol/cronos-general-faq, accessed 2026-08-31).

On the Cronos POS Chain, on which the crypto-asset is natively issued, participation is open. Any person may become a validator by bonding the crypto-asset and broadcasting the prescribed transaction, and the active set consists of the hundred validators with the largest bonded stake. Any holder may delegate to a validator of their choice. The issuer operates one validator node on that network and provides staking services in respect of the crypto-asset to third parties, receiving a share of the staking rewards generated. The issuer is accordingly one participant among the validators of that network and not its sole or controlling operator (source: https://www.sec.gov/Archives/edgar/data/2069288/000199937126010358/canarystaked-s1a_050826.htm, accessed 2026-08-31).

On 2026-08-30 the validator set of the Cronos EVM suspended block production on that network following an exploit of a lending protocol deployed on it, an action the project described as a validator-consensus emergency action. Block production on that network was resumed on 2026-08-31, the project stating that the chain state had been restored to a point preceding the exploit, with the effect that transactions recorded on that network in the intervening period were reversed. The Cronos POS Chain, on which the crypto-asset is natively issued, continued to produce blocks throughout.

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

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

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

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

5. Operational and information risks

A holder is unable to reverse a transfer of the crypto-asset once it has been recorded, and no counterparty is able to restore transferred units on a holder's instruction. Incorrect transaction approvals, or the use of a wrong network or a wrong address, will therefore typically make the transferred units irrecoverable. Because trading may also rely on technical connections to other venues or service providers, downtime or faulty code in these connections can temporarily block trading, deposits, or withdrawals even when the underlying blockchain is functioning. In addition,

different groups of market participants may have unequal access to technical, governance, or project-related information, which can lead to information asymmetry and place less informed investors at a disadvantage when making trading decisions.

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

Loss or theft of private keys, unauthorised access to wallets, or failures of custodial or exchange service providers can result in the irreversible loss of assets. A holder has no means of reversing a transfer or of compelling its reversal, so recovery of units following a compromise is generally impossible.

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

As this white paper relates to 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. Protocol, software and smart-contract vulnerability risk

The Cronos POS Chain protocol, client software, consensus components or other technical elements governing the native CRO crypto-asset may contain coding errors, implementation defects or security vulnerabilities. Exploitation or failure of these components could disrupt network operation, transaction processing or access to CRO and may result in loss of funds or other unintended consequences. In addition, where CRO is transferred, bridged or represented on other blockchain networks through smart contracts or bridge infrastructure, vulnerabilities in the relevant token contracts, bridge contracts, locking, minting or message-verification mechanisms may result in unauthorised transfers, unintended minting or burning, loss of assets, or inconsistencies between CRO representations across networks. Such vulnerabilities may persist despite testing, audits or other security measures.

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

Where a network operates a small or admission-controlled validator set, that set may be able to suspend block production across the entire network within a short period, and may be able to resume the network from an earlier state. A suspension halts all activity on the network, including positions and applications unconnected to the circumstances prompting it, and holders may be unable to transfer the crypto-asset for its duration. A restoration to an earlier state reverses transactions that were previously committed and treated as settled, which may affect holders who transacted in good faith in the intervening period and who have no means of preventing or contesting the reversal. Both occurred on the Cronos EVM network in August 2026.

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 crypto-asset

Cronos

S.4 Consensus Mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Solana and Osmosis. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Cronos POS:

Cronos POS Chain uses the CometBFT Proof-of-Stake consensus mechanism, based on the Tendermint BFT consensus protocol. Voting power is proportional to bonded CRO, comprising the validator's self-bonded stake and CRO delegated to it by holders. For each consensus round, a proposer is selected according to voting power and proposes a candidate block. Validators then proceed through the proposal, prevote and precommit stages. A block is committed and achieves deterministic finality once more than two-thirds of total voting power has precommitted to it, subject to the applicable Byzantine Fault Tolerance assumptions. Full nodes relay transactions and maintain and serve blockchain data but do not participate in block production unless they operate as active validators.

The following applies to Cronos EVM Chain:

Cronos EVM Chain secures its network with CometBFT (Tendermint-class) Byzantine Fault Tolerant consensus and a permissioned validator set, commonly described as a PoA-style variant of Proof-of-Stake. Designated validators propose and commit blocks in BFT rounds, and validator admission is by invitation under network governance. Safety holds provided fewer than one third of voting power is faulty or malicious. Blocks are final on commit, so there is no probabilistic confirmation period. Misbehaviour or insufficient liveness is penalised under protocol rules, including slashing for double-signing and jailing or tombstoning under the consensus parameters. Validators are expected to operate with high-availability infrastructure, redundancy, and standard network protections (for example DDoS mitigation). Finality on commit is a property of the consensus protocol and not a guarantee that the recorded state will be preserved. Where a sufficient share of voting power agrees to do so, the validator set is able to suspend block production and to resume it from an earlier state, with the effect that transactions previously committed and treated as final are reversed. This occurred on the network in August 2026.

The following applies to Ethereum:

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

The following applies to Cosmos (ATOM):

The Cosmos Hub operates a Proof-of-Stake (PoS) consensus mechanism based on CometBFT (formerly Tendermint consensus), a Byzantine Fault Tolerant (BFT) algorithm designed to provide fast finality and deterministic state replication.

Consensus participants are validators who bond the native crypto-asset ATOM as collateral and obtain voting power proportional to their bonded stake, including delegated ATOM from third parties. Validators participate in block production and consensus by proposing blocks and broadcasting cryptographic votes.

Consensus proceeds in rounds, each consisting of a block proposal, followed by two voting phases (pre-vote and pre-commit). A block is finalised and irreversibly committed once more than two-thirds of the total validator voting power pre-commits to the same block in the same round. This mechanism provides immediate finality and prevents probabilistic forks.

CometBFT ensures Byzantine Fault Tolerance, meaning the network remains safe and consistent as long as less than one-third of total voting power behaves maliciously or fails. The Cosmos Hub maintains a bounded validator set, initially capped at 100 validators and designed to increase gradually over time to balance decentralisation and performance.

The following applies to Solana:

Solana uses a combination of Proof-of-History (PoH) and Proof-of-Stake (PoS). The core concepts of the mechanism are intended to work as follows:

Core Concepts

1. Proof-of-History (PoH):

PoH is a cryptographic ordering and timing mechanism that provides evidence that data existed in a particular sequence and that time passed between proofs.

Verifiable Delay Function (VDF): PoH relies on a sequential hash-based proof process that Solana describes as VDF-like. This sequence of hashes provides a verifiable order of events, enabling the network to efficiently agree on the sequence of transactions.

2. Proof-of-Stake (PoS):

Validator Selection: Leader slots are assigned through the network's leader schedule, which is stake-weighted. The more SOL staked, the higher the chance of being selected to validate transactions and produce new blocks.

Delegation: Token holders can delegate their SOL tokens to validators, earning rewards proportional to their stake while contributing to the network's security.

Consensus Process

1. Transaction Validation:

Transactions are broadcasted to the network and collected by validators. Each transaction is validated to ensure it meets the network's criteria, such as having correct signatures and sufficient funds.

2. PoH Sequence Generation:

A validator generates a sequence of hashes using PoH, each containing a timestamp and the previous hash. This process creates a historical record of transactions, establishing a cryptographic clock for the network.

3. Block Production:

The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order.

4. Consensus and Finalisation:

Other validators vote on the ledger state associated with the block. A block may first become confirmed and later finalised once it reaches the network's strongest confirmation state.

Security and Economic Incentives

1. Incentives for Validators:

Block Rewards: Validators earn rewards for producing and validating blocks. These rewards are distributed in SOL tokens and are proportional to the validator's stake and performance.

Transaction Fees: Validators also earn transaction fees from the transactions included in the blocks they produce. These fees provide an additional incentive for validators to process transactions efficiently.

2. Security:

Staking: Staking provides economic alignment, and Solana documentation notes that slashing has been discussed as a future mechanism for intentional malicious behaviour, but is not implemented yet.

Delegated Staking: Token holders can delegate their SOL tokens to validators, intended to enhance network security and decentralisation. Delegators share in the rewards and are incentivised to choose reliable validators.

3. Economic Penalties:

Slashing (planned): Validators can be penalised for malicious behaviour, such as double-signing or producing invalid blocks. This penalty, known as slashing, results in the loss of a portion of the staked tokens, discouraging dishonest actions.

The following applies to Osmosis:

Osmosis operates a Proof-of-Stake consensus mechanism based on the Cosmos SDK and CometBFT, formerly Tendermint Core. CometBFT provides Byzantine Fault Tolerant state-machine

replication for application-specific blockchains and is designed to provide deterministic finality once the required validator voting threshold is reached.

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

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

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

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

S.5 Incentive Mechanisms and Applicable Fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Solana and Osmosis. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Cronos PoS Chain:

Cronos POS incentivises validators and delegators through staking rewards. Validators receive rewards based on bonded CRO, while CRO holders may delegate to validators and receive a share of the rewards after deduction of the validator's commission. Rewards comprise newly issued CRO and transaction fees; following the 2026 tokenomics upgrade, CRO emissions follow a governance-adjustable decay mechanism, while additional staking rewards may be funded from the dedicated rewards pool. Optional time-locked staking tiers provide additional rewards for longer-term commitments.

Validators are subject to penalties for consensus faults and insufficient liveness. Double-signing may result in slashing and permanent removal from validator participation, while extended downtime may result in slashing and temporary jailing. Delegated CRO is exposed to the same applicable slashing risk as the validator's stake.

The following applies to Cronos EVM Chain:

Validators on the Cronos EVM are remunerated from transaction fees paid in CRO. The validator set is permissioned and admission to it is by invitation, and CRO is not used for validator staking or for governance on that network. Fees are gas-based, being gas used multiplied by gas price, and are paid in CRO. A base fee is set for each block by the fee market module and adjusts upwards or downwards with network usage measured against a gas target. Fee parameters, including the base fee and the minimum gas price, are chain parameters and may be changed by governance.

The following applies to Ethereum:

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

The following applies to Cosmos (ATOM):

The Cosmos Hub secures its Proof-of-Stake consensus mechanism through an integrated system of economic incentives and penalties. This framework is designed to encourage honest participation by validators and delegators, deter malicious or negligent behaviour, and ensure the long-term security and sustainability of the network.

Incentive Mechanisms (Rewards)

Validators and delegators are rewarded for participating in block production and consensus through a combination of inflationary issuance and transaction fees. The native staking crypto-asset ATOM is issued as an inflationary reward and distributed to bonded validators and delegators in proportion to their bonded stake. In addition, users pay transaction fees, which are collected by validators and periodically redistributed to bonded participants, subject to validator-defined commission rates.

Transaction Fees

The Cosmos Hub applies a gas-based fee model to limit network spam and compensate network operators. Fees are calculated based on transaction complexity and size using a gas limit and a gas price, and are deducted from the transaction signer prior to execution. Validators may set their own minimum gas prices and may accept multiple token denominations as fees, selecting which transactions to include within block gas limits.

Fee Distribution and Reserve Pool

Collected transaction fees are redistributed at regular intervals to bonded validators and delegators in proportion to their bonded ATOM. A predefined portion of these fees (by default 2%) is allocated to a reserve pool, which is intended to support network security and sustainability and may be distributed through on-chain governance decisions.

Penalties and Slashing

Bonded ATOM functions as economic collateral and is subject to slashing in the event of protocol violations. Validators that commit safety faults, such as double-signing conflicting blocks at the same height, are subject to significant slashing and are typically permanently removed from the validator set.

The following applies to Solana:

1. Validators:

Validators participate in block production and voting under Solana's stake-weighted model. They may receive staking-related rewards and a share of transaction-fee income. Under Solana's fee model, the base fee is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This is intended to provide an additional financial incentive for validators to process transactions efficiently and maintain the network's integrity.

2. Delegators:

Delegated Staking: Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share the rewards earned by the validators. This is intended to encourage widespread participation in securing the network and to support decentralisation.

3. Economic Security:

Solana staking documentation notes slashing as a possible future mechanism for intentional malicious conduct, but states that slashing is not implemented in the protocol today. Economic alignment instead currently arises primarily from staking participation, validator performance incentives, and the opportunity cost of locking capital in staking positions.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana transactions require fees in SOL. The fee model consists of a base fee and, where used, an optional prioritisation fee. The base fee compensates signature verification work and is split between burn and validator compensation, while any prioritisation fee is paid to the validator.

2. Rent Fees:

Solana accounts that store on-chain state must satisfy the rent-exemption threshold, which is linked to the amount of data stored. This mechanism is intended to support efficient use of network state and account storage resources.

3. Program Execution Costs:

Deploying and interacting with on-chain programs may involve transaction fees and, where relevant, compute-related prioritisation fees and account-storage requirements. These mechanisms are intended to allocate network resources in proportion to use.

The following applies to Osmosis:

1. Validator and Delegator Rewards

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

2. Liquidity Provider Incentives

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

3. Transaction Fees

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

4. Slashing and Penalties

To discourage malicious or negligent behaviour, the protocol employs a bonded proof-of-stake model in which validators' staked assets may be subject to slashing. Validators that engage in protocol violations, such as double-signing, may incur a reduction of their staked assets. Validators

that fail to meet operational requirements, such as maintaining sufficient uptime, may be temporarily removed from the active validator set. Delegators are exposed to the risks associated with the validators to whom they delegate.

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

2025-01-17

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

2026-01-17

S.8 Energy consumption

109379.88888 kWh/a

S.9 Energy consumption sources and methodologies

The energy consumption associated with this crypto-asset is aggregated across multiple contributing components, primarily the underlying blockchain network and the execution of token-specific operations. To determine the energy consumption of a token, the energy consumption of the underlying blockchain networks Cronos PoS Chain, Cronos EVM Chain, Ethereum, Cosmos, Osmosis and Solana 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

33.3729184056 %

S.11 Energy intensity

0.00012 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

36.40306 tCO2e/a

S.14 GHG intensity

0.00005 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are determined using public information sites, open-source and in-house-developed crawlers. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal energy consumption with respect to one additional 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]. Underlying sources: Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: https://ourworldindata.org/grapher/share-electricity-renewables

S.16 Key GHG sources and methodologies

To determine GHG emissions, the locations of the nodes are determined using public information sites, open-source crawlers, and crawlers developed in-house. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal emission intensity with respect to one additional 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]. Underlying sources: Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: https://ourworldindata.org/grapher/carbon-intensity-electricity. Licensed under CC BY 4.0.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.