CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

# White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG 6C7F2WVZH

# Preamble

## 00. Table of Content

## 01. Date of notification

2026-01-08

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

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

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

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

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

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

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

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

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

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

## Summary

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

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

## 08. Characteristics of the crypto-asset

Cosmos ATOM (ATOM) is the crypto-asset described in this white paper and is classified as a crypto-asset other than an e-money token or an asset-referenced token. The crypto-asset is issued on the Cosmos Hub network (Cosmos chain), with representations issued on Binance Smart Chain, Ethereum, Cronos EVM, Osmosis, Injective and BitSong. The functionally fungible group digital token identifier (DTI FFG) is set out in Section F.14 of this white paper. The crypto-asset has no maximum supply and is subject to a variable issuance model; the initial supply at genesis was 236,198,958.12 ATOM units. The crypto-asset is issued natively on Cosmos Hub and is represented on other networks under the following technical standards: Cosmos (native crypto-asset), Binance Smart Chain (BEP-20), Ethereum (ERC-20), Cronos EVM (CRC-20), Osmosis (IBC coin), Injective (IBC coin) and BitSong (IBC coin). The first on-chain activity on Cosmos Hub occurred on 2019-03-13 in block 1 (block hash 0D9BB9FA6EB9D64E80CF920EB917B1124F298B12C92BE7FD5328564C6D85D087), available at https://www.mintscan.io/cosmos/block/1?chainId=cosmoshub-1, accessed on 2026-01-07; the first on-chain activity on Binance Smart Chain occurred on 2020-09-14 (transaction hash fa763455b540705486499f337a12eeee5efcb72f18b1d667a9719eca860e0c69), available at https://bscscan.com/tx/0xfa763455b540705486499f337a12eeee5efcb72f18b1d667a9719eca860e0c69, accessed on 2026-01-07; the first on-chain activity on Ethereum occurred on 2021-09-05 (transaction hash f1529ea5dd14789af2ba96d4dd7370a940cdf185ab33a12f5feadb04d6b84fb0), available at https://etherscan.io/tx/0xf1529ea5dd14789af2ba96d4dd7370a940cdf185ab33a12f5feadb04d6b84fb0, accessed on 2026-01-07; the first on-chain activity on Osmosis occurred on 2021-06-19 (IBC channel activity at https://www.mintscan.io/osmosis/relayers/channel-0/cosmos/channel-141), accessed on 2026-01-07; the first on-chain activity on Injective occurred on 2021-10-25 (IBC channel activity at https://www.mintscan.io/injective/relayers/channel-1/cosmos/channel-220), accessed on 2026-01-07; the first on-chain activity on Cronos EVM occurred on 2021-12-13 (transaction hash a656273fdd6fe63e826d79b4f7614e3c6952b53a7f3f24b5e8e96bdeba6dd257), available at https://explorer.cronos.org/tx/0xa656273fdd6fe63e826d79b4f7614e3c6952b53a7f3f24b5e8e96bdeba6dd257, accessed on 2026-01-07; the first on-chain activity on BitSong could not be identified on the basis of the available information.

Cosmos is a decentralised network designed to enable interoperability between independent blockchains through an architecture that distinguishes between hubs and zones and uses inter-chain communication to transmit information and crypto-assets across connected networks. The Cosmos Hub is the first hub in this ecosystem and ATOM is the crypto-asset used within the Cosmos Hub for operational purposes, including participation in network security through staking, payment of network fees for transactions on the Cosmos Hub, and participation in governance processes relating to changes and parameters within the Cosmos Hub.

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

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

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

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

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

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

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

### A.1 Name

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

### A.2 Legal form

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

### A.3 Registered address

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

Germany,

federal state Hamburg.

### A.4 Head office

Crypto Risk Metrics GmbH has no head office.

### A.5 Registration date

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

### A.6 Legal entity identifier

39120077M9TG0O1FE242

### A.7 Another identifier required pursuant to applicable national law

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

### A.8 Contact telephone number

+4915144974120

### A.9 E-mail address

info@crypto-risk-metrics.com

### A.10 Response time (Days)

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

### A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

### A.12 Members of the management body

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

### A.13 Business activity

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

### A.14 Parent company business activity

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

### A.15 Newly established

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

### A.16 Financial condition for the past three years

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

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

2024 (unaudited): negative EUR 50.891,81

2023 (unaudited): negative EUR 27.665,32

2022: EUR 104.283,00.

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

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

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

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

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

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

### A.17 Financial condition since registration

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

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

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

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

### B.2 Name

Interchain Foundation

## B.3 Legal form

The legal form of Interchain Foundation is 2JZ4, which corresponds to "Foundation".

## B4. Registered address

The registered address of Interchain Foundation is Gartenstrasse 4, 6300 Zug

Switzerland,

ZG

## B.5 Head office

The Head Office address of Interchain Foundation is Gartenstrasse 4, 6300 Zug

Switzerland,

ZG

## B.6 Registration date

Interchain Foundation was registered on 2017-03-07.

## B.7 Legal entity identifier

50670084O45T1JISE389

## B.8 Another identifier required pursuant to applicable national law

CHE-199.569.367

## B.9 Parent company

No parent company of Interchain Foundation can be identified.

## B.10 Members of the management body

| Identity | Function | Business Address |
|---|---|---|
| Josh Cincinnati | Chairperson of the foundation board | Gartenstrasse 4, 6300 Zug, Switzerland |
| Maxime Monod | Vice-chairperson of the foundation board | Gartenstrasse 4, 6300 Zug, Switzerland |
| Dirk Steller | member of the foundation board | Gartenstrasse 4, 6300 Zug, Switzerland |

## B.11 Business activity

Promotion and development of new technologies and applications, in particular in the areas of new open and decentralized software architectures; with primary focus — but not exclusively — on the promotion and development of the Cosmos network, the Polkadot protocol, and the corresponding technologies, as well as the procurement of the necessary funds through contributions from third parties; full statement of purpose as set out in the foundation deed.

## B.12 Parent company business activity

Interchain Foundation does not have a parent company. Accordingly, no business activity of a parent company is to be reported in this section.

## 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: "Cosmos ATOM", Short Name: "ATOM" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-01-08).

### D.2 Crypto-assets name

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

### D.3 Abbreviation

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

### D.4 Crypto-asset project description

According to public information (source: https://docs.cosmos.network/, accessed 2026-01-07), the Cosmos ecosystem is a crypto-asset initiative concerned with the development and maintenance of a decentralised software framework intended to support the operation of multiple independent distributed-ledger networks. The ecosystem is designed around a "Hub and Zone" architecture, in which application-specific blockchains ("Zones") may connect to coordination blockchains ("Hubs") in order to facilitate the exchange of data and crypto-assets. The technical framework is based on several software components, including the Cosmos SDK, a modular development framework for building distributed-ledger applications; CometBFT, a Byzantine Fault Tolerant Proof-of-Stake consensus engine responsible for networking and block finalisation; and the Inter-Blockchain Communication (IBC) protocol, which provides a standardised method for exchanging messages and assets between compatible blockchains using cryptographic verification mechanisms.

Within this framework, the Cosmos Hub operates as one possible coordination blockchain for connected zones and may support additional mechanisms for validator coordination and shared security, subject to technical configuration and governance decisions. The Cosmos ecosystem also includes optional execution environments, including Ethereum-compatible virtual machine implementations, which may allow smart contract deployment on certain Cosmos-based chains. The availability, performance, and interoperability of these components depend on the continued operation of the underlying software, validator participation, governance outcomes, and the technical compatibility of participating networks.

The ATOM crypto-asset functions as the native network-participation and coordination instrument of the Cosmos Hub within this technical environment. ATOM may be used to support validator participation through staking and delegation mechanisms, to take part in on-chain governance processes, and to pay transaction fees on the Cosmos Hub, subject to applicable protocol rules. The economic design of ATOM includes a variable issuance mechanism intended to incentivise validator participation by targeting a defined proportion of bonded crypto-assets. Certain features, including staking rewards, delegated penalties for validator misconduct, liquid staking arrangements, and the use of ATOM in connection with interchain security mechanisms, depend on protocol parameters, governance decisions, and ongoing technical implementation and may be modified, restricted, or discontinued.

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

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

| Type of person | Name of person | Business address of person | Domicile of company |
|---|---|---|---|
| Other person involved in implementation | Jae Kwon | Can not be found | Can not be found |
| Other person involved in implementation | Ethan Buchman | Can not be found | Can not be found |
| Other person involved in implementation | Interchain Foundation (ICF) | Gartenstrasse 4, 6300 Zug, Switzerland | Switzerland |
| Other person involved in implementation | Josh Cincinnati | Gartenstrasse 4, 6300 Zug, Switzerland | Switzerland |
| Other person involved in implementation | Maxime Monod | Gartenstrasse 4, 6300 Zug, Switzerland | Switzerland |
| Other person involved in implementation | Dirk Steller | Gartenstrasse 4, 6300 Zug, Switzerland | Switzerland |
| Other person involved in implementation | All in Bits, Inc | 3395 S Jones Blvd, Las Vegas, Nevada, United States | United States |
| Other person involved in implementation | Cosmos Labs | 740 Broadway, STE 1002, New York City, 10003, NY, USA | United States |

| Type of person | Name of person | Business address of person | Domicile of company |
|---|---|---|---|
| Other person involved in implementation | Barry Plunkett | 740 Broadway, STE 1002, New York City, 10003, NY, USA | United States |
| Other person involved in implementation | Maghnus Mareneck | 740 Broadway, STE 1002, New York City, 10003, NY, USA | United States |
| Other person involved in implementation | Cosmos Labs GmbH | Donaustr. 44, D-12043 Berlin | Germany |
| Other person involved in implementation | Anna-Julia Schmauser | Donaustr. 44, D-12043 Berlin | Germany |

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

There is no formally published multi-year roadmap for the ATOM crypto-asset. Based on public information (sources: https://www.cosmoslabs.io/blog/the-cosmos-stack-roadmap-2026 accessed 2025-01-07; https://www.cosmoslabs.io/ accessed 2025-01-07; Cosmos Hub governance forum materials and Interchain Foundation engineering updates accessed 2026-01-07), several protocol upgrades, ecosystem initiatives, and ATOM-related developments have been communicated that affect the evolution of the Cosmos Hub and broader Cosmos Stack, and may influence the economic role and market dynamics of the ATOM crypto-asset.

Past milestones:

- Tendermint Development Initiation (2014): Early technical work on Tendermint consensus began, forming part of the research and engineering foundation later used in the Cosmos Stack and the Cosmos Hub, where ATOM is used for staking and governance processes.

- Interchain Foundation Fundraiser and Genesis Allocation Framework (April 2017): A public fundraiser associated with the ecosystem was conducted, with public materials commonly referencing a genesis allocation of 236,198,958.12 ATOM and related distribution parameters.

- Cosmos Hub Mainnet Launch (March 13, 2019): The Cosmos Hub mainnet went live, enabling initial on-chain staking, validator operations, and governance for ATOM in a production environment.

- IBC Enablement on the Cosmos Hub (February 2021): The Stargate upgrade period enabled IBC capabilities on the Cosmos Hub, establishing the technical basis for interchain messaging and transfers.

- Theta Upgrade (Q1 2022): Introduced Interchain Accounts and the first iteration of Liquid Staking, allowing users to maintain liquidity while earning staking rewards. This upgrade expanded the economic utility of ATOM and enhanced user engagement within the interchain ecosystem.

- Onboarding of First Consumer Chains (2023): The Cosmos Hub successfully onboarded its first two consumer chains via Interchain Security: Neutron (May 2023) and Stride (July 2023), demonstrating the scalability and real-world applicability of the ATOM-based security model.

- Phase 1 of ATOM Tokenomics Redesign (Late 2025): Cosmos Labs announced a three-phase initiative to realign ATOM's value with enterprise adoption of the Cosmos SDK. Phase 1 (Audit) involves benchmarking ATOM usage against competitors such as Avalanche and ZKSync, with a research proposal deadline set for January 15, 2026.

Future milestones:

- Phase 2 of ATOM Tokenomics Redesign (2026): This phase will focus on modeling supply, demand, and inflation scenarios, including potential mechanisms for generating revenue for ATOM holders through SDK licensing or usage fees. These models will inform governance proposals under community review.

- Phase 3 of ATOM Tokenomics Redesign (2026): Community-driven governance proposals will be codified to implement the redesigned tokenomics. The goal is to link ATOM's value more directly to the economic activity and enterprise adoption of the Cosmos SDK.

- Q1/Q2 2026: Implementation of Native Proof of Authority (PoA), BLS signing, and BlockSTM to improve efficiency and transaction throughput, supporting the Hub's scalability and performance goals.

- Q2 2026: Expansion of first-class IBC connectivity to Solana and Ethereum Layer 2 networks, increasing the ecosystem's interoperability and adoption potential.

- Q4 2026: Targeting a production reality of 5,000 TPS and 500ms block times across geographically distributed validator sets, representing a significant performance upgrade for the Cosmos Hub.

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 performance or implementation does not guarantee future success, and changes may materially affect the value or utility of the ATOM token for holders.

### D.9 Resource allocation

According to publicly available information found at https://github.com/cosmos/cosmos/blob/master/PLAN.md (accessed on 2025-01-07), the ATOM crypto-asset was initially minted during a public fundraiser held on April 6, 2017, under the stewardship of the Interchain Foundation (ICF) to fund the development of a decentralized, interoperable network. A total of 236,198,958.12 ATOM tokens were recommended for genesis allocation, distributed across 984 accounts, with the majority allocated to public contributors, and the remainder reserved for strategic stakeholders, early adopters, and development entities.

At the time of the fundraiser, 160,293,050 ATOM (67.9% of the total genesis supply) were allocated to Public Contributors. Seed Contributors, the earliest financial backers, received 11,809,947.91 ATOM (5%). Strategic contributors received 16,856,718.97 ATOM (7.1%). The Interchain Foundation (ICF) received 23,619,895.81 ATOM (10%) to fund ongoing research and development, while All in Bits, Inc. (AiB, the original developer of the Tendermint consensus protocol) received an equal allocation of 23,619,895.81 ATOM (10%) to support open-source IP development and maintain the network's infrastructure.

While most allocations were immediately available and unrestricted, tokens allocated to AiB were subject to vesting conditions: 1,777,707 ATOM were locked for 12 months, and the remaining 21,842,188.81 ATOM were subject to monthly vesting over 22 months, beginning two months after network launch.

### 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 ATOM token has no maximum supply and is designed as an inflationary asset, with its total supply dynamically adjusted based on the network's staking participation and ongoing tokenomics redesigns. The current circulation supply (486,982,674 units as of 2025-01-07) can be traced here: https://www.mintscan.io/cosmos/

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 gas fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

## E.37 Offer expenses

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

## E.38 Conflicts of interest

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

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

## E.39 Applicable law

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

### E.40 Competent court

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

## Part F – Information about the crypto-assets

### F.1 Crypto-asset type

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

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

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

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

### F.2 Crypto-asset functionality

According to public information available in the Cosmos Hub documentation (https://docs.cosmos.network/, accessed 2026-01-07) and associated governance resources, the ATOM token is the native on-chain crypto-asset of the Cosmos Hub and is used for protocol-level participation in network security and on-chain governance. ATOM holders can delegate (stake) ATOM to validators to help secure the Cosmos Hub and, in return, participate in the distribution of protocol-defined rewards.

ATOM's core functionality is staking-based security coordination. The Cosmos Hub maintains an active validator set (configured via on-chain parameters), and ATOM holders who do not operate validator infrastructure can participate as delegators by bonding ATOM to a chosen validator.

ATOM also enables decentralized decision-making through on-chain governance on the Cosmos Hub. Bonded ATOM holders can submit, deposit on, and vote on governance proposals, including parameter changes, community pool spending decisions, and software upgrades. A delegator's voting power is proportional to their bonded stake.

Within the Cosmos Hub, ATOM is used as the accounting basis for validator and delegator incentives. Rewards are described in the Hub documentation as (i) block provisions paid in newly created ATOM under a dynamic inflation mechanism targeting a two-thirds bonded ratio (with inflation bounded between 7% and 20% in the referenced documentation), and (ii) transaction fees that may be paid in governance-whitelisted denominations and distributed to bonded ATOM holders proportionally. In addition, the Hub documentation describes the Liquid Staking Module (LSM), which allows tokenization of staked positions into transferable "LSM shares," enabling "instant" conversion of already-staked ATOM into a form usable by liquid staking providers without waiting through the unbonding period.

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

## F.3 Planned application of functionalities

The project's public documentation outlines additional functionalities that may be introduced in future protocol upgrades:

Future milestones:

- Phase 2 of ATOM Tokenomics Redesign (2026): This phase will focus on modeling supply, demand, and inflation scenarios, including potential mechanisms for generating revenue for ATOM holders through SDK licensing or usage fees. These models will inform governance proposals under community review.

- Phase 3 of ATOM Tokenomics Redesign (2026): Community-driven governance proposals will be codified to implement the redesigned tokenomics. The goal is to link ATOM's value more directly to the economic activity and enterprise adoption of the Cosmos SDK.

- Q1/Q2 2026: Implementation of Native Proof of Authority (PoA), BLS signing, and BlockSTM to improve efficiency and transaction throughput, supporting the Hub's scalability and performance goals.

- Q2 2026: Expansion of first-class IBC connectivity to Solana and Ethereum Layer 2 networks, increasing the ecosystem's interoperability and adoption potential.

- Q4 2026: Targeting a production reality of 5,000 TPS and 500ms block times across geographically distributed validator sets, representing a significant performance upgrade for the Cosmos Hub.

These functionalities remain conditional on future development, audit completion, and governance approval. No assurance is given regarding their eventual activation, scope, or long-term availability.

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

### F.4 Type of crypto-asset white paper

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

### F.5 The type of submission

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

### F.6 Crypto-asset characteristics

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

### F.7 Commercial name or trading name

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

### F.8 Website of the issuer

https://interchain.io/

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

2026-02-06

### F.10 Publication date

2026-02-06

### 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

J51DXB76N, 6453368PD, W03RCK39H, HX1NSP98N, MC73KT6K4, 2RZ13PHH3, JVMWS68W1, DJ0QPRH0W

### F.14 Functionally fungible group digital token identifier

6C7F2WVZH

### F.15 Voluntary data flag

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

### F.16 Personal data flag

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

### F.17 LEI eligibility

The issuer 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 claim capable of legal enforcement against the issuer or any third party.

### G.2 Exercise of rights and obligations

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

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

## G.3 Conditions for modifications of rights and obligations

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

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

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

## G.4 Future public offers

Information on the future offers to the public of crypto-assets were not available at the time of writing this white paper (2026-01-07).

## G.5 Issuer retained crypto-assets

According to publicly available information found at https://github.com/cosmos/cosmos/blob/master/PLAN.md (accessed on 2025-01-07), the ATOM token allocation includes 23,619,895.81 ATOM allocated to the Interchain Foundation (ICF) and an equal allocation of 23,619,895.81 ATOM allocated to All in Bits, Inc. (AiB), representing 10% each of the total genesis supply. These allocations together total 47,239,791.62 ATOM and form part of the initial reserve held by strategic stakeholders and core protocol developers.

Note: While the combined allocation to the Interchain Foundation and All in Bits, Inc. is publicly disclosed, on-chain wallet addresses associated with these allocations cannot be independently linked to specific natural persons or legal entities. Token movements or internal treasury management actions may occur without prior notice and could affect the concentration of holdings and the future governance influence associated with these assets. The current token distribution can be traced on-chain: https://www.mintscan.io/cosmos/assets/uatom?sector=holders.

## 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 is no fixed, demand-responsive protocol that increases or decreases the supply of the ATOM crypto-asset in response to changes in demand.

However, the ATOM crypto-asset is designed as an inflationary crypto-asset with no maximum supply. At genesis (April 6, 2017), the initial supply was 236,198,958.12 ATOM, and the supply may increase over time through continuous minting of new ATOM as rewards for validators and delegators participating in the Proof-of-Stake consensus mechanism. The inflation rate is dynamic and determined by an automated protocol that adjusts based on the proportion of the total supply that is staked (the “bonded ratio”), with a target staking level of approximately two-thirds (about 67%). Historically, this mechanism was designed to operate within an inflation range of 7% (minimum) to 20% (maximum), increasing inflation when the bonded ratio falls below the target and decreasing inflation when the bonded ratio exceeds the target. More recently, inflation has been observed to fluctuate in a narrower range of approximately 7% to 10%, depending on staking participation.

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

The ATOM crypto-asset is designed as an inflationary crypto-asset with no maximum supply. Investors should note that changes in the supply of the crypto-asset can have a negative impact.

### G.14 Token value protection schemes

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

### G.15 Token value protection schemes description

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

### G.16 Compensation schemes

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

### G.17 Compensation schemes description

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

### G.18 Applicable law

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

### G.19 Competent court

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

## Part H – information on the underlying technology

### H.1 Distributed ledger technology (DTL)

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

### H.2 Protocols and technical standards

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

The following applies to Cosmos:

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 Binance Smart Chain:

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

The following applies to Ethereum:

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

1. Network Protocols

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

- Transactions and smart contract execution are secured through Proof-of-Stake (PoS) consensus.

- Validators propose and attest blocks in Ethereum's Beacon Chain, finalized through Casper FFG.

- The Ethereum Virtual Machine (EVM) executes smart contracts using Turing-complete bytecode.

2. Transaction and Address Standards

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

Transaction Types:

- Legacy Transactions (pre-EIP-1559)

- Type 0 (Pre-EIP-1559 transactions)

- Type 1 (EIP-2930: Access list transactions)

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

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

3. Blockchain Data Structure & Block Standards

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

Each block contains:

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

- Transactions: Smart contract executions and token transfers.

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

4. Upgrade & Improvement Standards

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

The following applies to Cronos EVM:

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 validator set is permissioned under network governance (commonly described as a PoA-style variant of Proof-of-Stake): designated validators propose and commit blocks; token holders may participate indirectly via delegation where enabled by protocol/governance. Finality occurs on block commit subject to consensus parameters and validator participation. The protocol is open-source and maintained in public repositories.

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 (e.g., legacy/type-0 and, if enabled by chain parameters, access-list/type-1 and dynamic-fee/type-2). Fee mechanics are chain-parameterized; no representation is made that Ethereum's base-fee burning rules apply on Cronos EVM Chain.

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. State storage and proofs follow the Ethereum account/state-trie model as implemented in Ethermint. Effective block capacity is bounded by gas limits and consensus parameters rather than a fixed byte size.

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.

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 Osmosis:

Osmosis is built on the Cosmos SDK and uses the Inter-Blockchain Communication (IBC) protocol for interoperability. These standards enable cross-chain interaction within the Cosmos ecosystem but remain dependent on the adoption and stability of the Cosmos framework. Reliance on a still-developing interoperability standard may introduce integration and security risks.

The following applies to Injective:

Injective is built on the Cosmos SDK and uses the Inter-Blockchain Communication (IBC) protocol for interoperability. These standards enable cross-chain interaction within the Cosmos ecosystem but remain dependent on the adoption and stability of the Cosmos framework. Reliance on a still-developing interoperability standard may introduce integration and security risks.

The following applies to BitSong:

BitSong is built on the Cosmos SDK and uses the Inter-Blockchain Communication (IBC) protocol for interoperability. These standards enable cross-chain interaction within the Cosmos ecosystem but remain dependent on the adoption and stability of the Cosmos framework. Reliance on a still-developing interoperability standard may introduce integration and security risks.

### H.3 Technology used

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

The following applies to Cosmos:

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 Binance Smart Chain:

1. BSC-Compatible Wallets

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

2. Ledger

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

3. BEP-20 Token Standard

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

4. Scalability and Transaction Efficiency

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

The following applies to Ethereum:

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

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

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

The following applies to Cronos EVM:

1. Decentralized Ledger

Cronos EVM Chain is a public, EVM-compatible Layer-1 built with the Cosmos SDK and Ethermint, with consensus provided by CometBFT (Tendermint-class BFT). It records transactions in CRO on a transparent, append-only ledger. Blocks are finalized upon commit under the BFT protocol, subject to network parameters and validator participation.

2. Private Key Management

Users interact via EVM-compatible wallets (e.g., MetaMask, Ledger, Crypto.com DeFi Wallet in EVM mode). 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). State and execution follow the EVM account/storage trie model as implemented by Ethermint, enabling standard Ethereum proofs and verification semantics.

4. Consensus and Security

Cronos EVM Chain runs a BFT consensus with a permissioned validator set (commonly described as a PoA-style variant of Proof-of-Stake). Security assumptions tolerate up to one-third faulty or malicious voting power without breaking safety. Validators are expected to operate with high-availability infrastructure, redundancy, and standard network protections (e.g., DDoS mitigation). Gas fees are paid in CRO; finality and throughput depend on consensus parameters, validator performance, and network conditions.

The following applies to Osmosis:

The platform functions as an automated market maker (AMM) with customizable liquidity pools. Osmosis leverages the Tendermint Core consensus engine and Cosmos SDK modules, which provide modularity and extensibility. While this design supports innovation, it also increases the attack surface, and the AMM model itself remains sensitive to issues such as front-running, slippage, and smart contract vulnerabilities.

The following applies to Injective:

Injective is built on a modular, high-performance blockchain architecture designed to power next-generation DeFi applications. It leverages the Cosmos SDK and Tendermint Core BFT consensus engine to deliver scalability, security, and interoperability — while maintaining a flexible, extensible framework for developers.

The platform supports a suite of native modules tailored for DeFi use cases, including decentralized exchanges, derivatives trading, oracles, and cross-chain asset transfers. These modules operate through the Cosmos SDK's application interface (ABCI), enabling developers to build and deploy complex financial applications without modifying the underlying consensus or networking layers.

Injective's architecture is further enhanced by its MultiVM environment, supporting smart contracts across WASM, EVM, and SVM, allowing seamless deployment of existing DeFi logic and enabling broader developer adoption.

While this modular design accelerates innovation and customization, it also introduces additional complexity — and with it, an expanded attack surface compared to monolithic chains.

The following applies to BitSong:

BitSong's primary goal is to enable music-focused applications (e.g., music streaming services, Fan Tokens and NFTs) on an application-specific Layer-1 blockchain. Bitsong leverages the CometBFT consensus engine and Cosmos SDK modules, which provide modularity and extensibility. While this design supports innovation, it also increases the attack surface.

## H.4 Consensus mechanism

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

The following applies to Cosmos:

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 finalized 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 decentralization and performance.

The following applies to Binance Smart Chain:

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

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

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

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

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

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

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

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

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

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

The following applies to Ethereum:

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

The following applies to Cronos EVM:

Cronos EVM 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; where enabled by governance, CRO holders may participate indirectly via delegation to validators and share in fee- or reward-based distributions as defined by on-chain parameters. Rewards, if configured, derive from protocol emissions and transaction fees paid in CRO; fees are gas-based (gas used × gas price) and their mechanics (e.g., dynamic-fee support, any base-fee logic) are chain-parameterized rather than guaranteed to mirror Ethereum’s EIP-1559/burning model. Misbehavior or insufficient liveness can be penalized per protocol rules (e.g., slashing for double-signing, jailing/tombstoning per consensus parameters). The incentive design targets rapid finality and predictable execution costs, with security aligned to validator performance, governance settings, and stake configuration.

The following applies to Osmosis:

Osmosis applies a Proof-of-Stake consensus through the Tendermint BFT engine. Validator nodes secure the network by staking OSMO tokens, and consensus is reached with fast finality. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behavior. The system may be exposed to validator collusion or governance capture.

The following applies to Injective:

Injective applies a Proof-of-Stake consensus through the Tendermint BFT engine. Validator nodes secure the network by staking INJ tokens, and consensus is reached with fast finality. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behavior. The system may be exposed to validator collusion or governance capture.

The following applies to BitSong:

BitSong applies a delegated Proof-of-Stake model using a Tendermint-style BFT engine (CometBFT/Tendermint lineage). Validator nodes secure the network by bonding BTSG (including BTSG delegated by other holders), propose/validate blocks, and earn protocol rewards. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behavior. The system may be exposed to validator collusion or governance capture.

### H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

The following applies to Cosmos:

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 behavior, 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 Binance Smart Chain:

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

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

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

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

4. Economic Security: Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network. Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets. Fees on the Binance Smart Chain

5. Transaction Fees: Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators. Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.

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

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

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

The following applies to Ethereum:

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

The following applies to Cronos EVM:

Cronos EVM 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; where enabled by governance, CRO holders may participate indirectly via delegation to validators and share in fee- or reward-based distributions as defined by on-chain parameters. Rewards, if configured, derive from protocol emissions and transaction fees paid in CRO; fees are gas-based (gas used × gas price) and their mechanics (e.g., dynamic-fee support, any base-fee logic) are chain-parameterized rather than guaranteed to mirror Ethereum’s EIP-1559/burning model. Misbehavior or insufficient liveness can be penalized per protocol rules (e.g., slashing for double-signing, jailing/tombstoning per consensus parameters). The incentive design targets rapid finality and predictable execution costs, with security aligned to validator performance, governance settings, and stake configuration.

The following applies to Osmosis:

The network incentivizes liquidity providers and validators through block rewards and transaction fees paid in OSMO. Liquidity mining programs and governance-driven reward distribution may influence participation but can also result in centralization of liquidity or speculative behavior. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

The following applies to Injective:

The network incentivizes liquidity providers and validators through block rewards and transaction fees paid in INJ. Liquidity mining programs and governance-driven reward distribution may influence participation but can also result in centralization of liquidity or speculative behavior. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

The following applies to BitSong:

BitSong incentivizes validators and delegators through (i) block rewards funded by newly-minted BTSG under an inflation algorithm that adjusts based on the share of BTSG that is bonded/staked, and (ii) transaction fees paid in BTSG, which flow into reward pools and are distributed to validators and delegators (net of validator commission). Misbehavior and operational faults are discouraged through slashing and jailing (e.g., penalties for double-signing and downtime, with chain parameters defining the penalty fractions and jail duration). Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

### H.6 Use of distributed ledger technology

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

### H.7 DLT functionality description

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

### H.8 Audit

Since the question of "technology" is understood in a broad sense, the answer to the question of whether an examination of the "technology used" has been carried out is "no, we cannot guarantee that all parts of the technology used have been examined." This is because this report focuses on risks and we cannot guarantee that every part of the technology used has been examined.

### H.9 Audit outcome

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

## Part I – Information on risks

### I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service-provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

### I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

### I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

## I.4 Project implementation-related risks

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

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

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

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

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

### I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

### I.6 Mitigation measures

None.

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

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

### S.1 Name

Crypto Risk Metrics GmbH

### S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

### S.3 Name of the cryptoasset

Cosmos ATOM

### S.4 Consensus Mechanism

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

The following applies to Cosmos:

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 finalized 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 decentralization and performance.

The following applies to Binance Smart Chain:

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

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

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

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

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

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

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

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

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

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

The following applies to Ethereum:

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

The following applies to Cronos EVM:

Cronos EVM 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; where enabled by governance, CRO holders may participate indirectly via delegation to validators and share in fee- or reward-based distributions as defined by on-chain parameters. Rewards, if configured, derive from protocol emissions and transaction fees paid in CRO; fees are gas-based (gas used × gas price) and their mechanics (e.g., dynamic-fee support, any base-fee logic) are chain-parameterized rather than guaranteed to mirror Ethereum's EIP-1559/burning model. Misbehavior or insufficient liveness can be penalized per protocol rules (e.g., slashing for double-signing, jailing/tombstoning per consensus parameters). The incentive design targets rapid finality and predictable execution costs, with security aligned to validator performance, governance settings, and stake configuration.

The following applies to Osmosis:

Osmosis applies a Proof-of-Stake consensus through the Tendermint BFT engine. Validator nodes secure the network by staking OSMO tokens, and consensus is reached with fast finality. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behavior. The system may be exposed to validator collusion or governance capture.

The following applies to Injective:

Injective applies a Proof-of-Stake consensus through the Tendermint BFT engine. Validator nodes secure the network by staking INJ tokens, and consensus is reached with fast finality. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behavior. The system may be exposed to validator collusion or governance capture.

The following applies to BitSong:

BitSong applies a delegated Proof-of-Stake model using a Tendermint-style BFT engine (CometBFT/ Tendermint lineage). Validator nodes secure the network by bonding BTSG (including BTSG delegated by other holders), propose/validate blocks, and earn protocol rewards. While PoS ensures efficiency, the validator set is comparatively small, creating concentration risks and dependence on correct governance behavior. The system may be exposed to validator collusion or governance capture.

### S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is implemented on the Cosmos blockchain, Binance Smart Chain, Ethereum, Cronos EVM chain, Osmosis, Injective and BitSong networks following the standards described below.

The following applies to Cosmos:

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 behavior, 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 Binance Smart Chain:

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

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

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

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

4. Economic Security: Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network. Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets. Fees on the Binance Smart Chain

5. Transaction Fees: Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators. Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet.

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

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

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

The following applies to Ethereum:

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

The following applies to Cronos EVM:

Cronos EVM 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; where enabled by governance, CRO holders may participate indirectly via delegation to validators and share in fee- or reward-based distributions as defined by on-chain parameters. Rewards, if configured, derive from protocol emissions and transaction fees paid in CRO; fees are gas-based (gas used × gas price) and their mechanics (e.g., dynamic-fee support, any base-fee logic) are chain-parameterized rather than guaranteed to mirror Ethereum's EIP-1559/burning model. Misbehavior or insufficient liveness can be penalized per protocol rules (e.g., slashing for double-signing, jailing/tombstoning per consensus parameters). The incentive design targets rapid finality and predictable execution costs, with security aligned to validator performance, governance settings, and stake configuration.

The following applies to Osmosis:

The network incentivizes liquidity providers and validators through block rewards and transaction fees paid in OSMO. Liquidity mining programs and governance-driven reward distribution may influence participation but can also result in centralization of liquidity or speculative behavior. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

The following applies to Injective:

The network incentivizes liquidity providers and validators through block rewards and transaction fees paid in INJ. Liquidity mining programs and governance-driven reward distribution may influence participation but can also result in centralization of liquidity or speculative behavior. Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

The following applies to BitSong:

BitSong incentivizes validators and delegators through (i) block rewards funded by newly-minted BTSG under an inflation algorithm that adjusts based on the share of BTSG that is bonded/staked, and (ii) transaction fees paid in BTSG, which flow into reward pools and are distributed to validators and delegators (net of validator commission). Misbehavior and operational faults are discouraged through slashing and jailing (e.g., penalties for double-signing and downtime, with chain parameters defining the penalty fractions and jail duration). Fees are variable, and long-term sustainability depends on balancing incentives with network security and cost efficiency.

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

2025-01-08

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

2026-01-08

### S.8 Energy consumption

186482.44055 kWh/a

### S.9 Energy consumption sources and methodologies

The energy consumption of this asset is aggregated across multiple components:

For the calculation of energy consumptions, the so called 'bottom-up' approach is being used. The nodes are considered to be the central factor for the energy consumption of the network. These assumptions are made on the basis of empirical findings through the use of public information sites, open-source crawlers and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the client software. The energy consumption of the hardware devices was measured in certified test laboratories. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset of question in scope and we update the mappings regulary, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

To determine the energy consumption of a token, the energy consumption of the underlying blockchain networks 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

33.8173640925 %

### S.11 Energy intensity

0.00011 kWh

### S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

### S.13 Scope 2 DLT GHG emissions – Purchased

62.06379 tCO2e/a

### S.14 GHG intensity

0.00004 kgCO2e

### S.15 Key energy sources and methodologies

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

### S.16 Key GHG sources and methodologies

To determine the GHG Emissions, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal emission wrt. one more transaction. Ember (2025); Energy Institute -

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.