CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG M7NN4STH9

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified on 2026-06-08.

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 omission likely to affect its import.

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

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

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

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

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

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

Summary

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

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

08. Characteristics of the crypto-asset

The crypto-asset TIA referred to in this white paper is a crypto-asset other than EMTs and ARTs and is native to the Celestia blockchain and is also available on the Osmosis and Injective networks, according to the DTI FFG shown in section F.14, as of 2026-06-03. The initial supply of the crypto-asset was set to 1 000 000 000 tokens. TIA has an inflationary supply model under which new TIA is issued over time to support staking rewards and network security. According to public information, the protocol was launched with an annual inflation rate of 8%, which has subsequently been reduced through protocol upgrades. As of the v6 upgrade, the annual inflation rate is approximately 2.5% and is expected to continue declining over time until it reaches a long-term floor of 1.5%. The first mined block on the Celestia network can be viewed on 2023-10-31 (block hash: 6BE39EFD10BA412A9DB5288488303F5DD32CF386707A5BEF33617F4C43301872, source: https://celenium.io/block/1, accessed 2026-06-03). The first activity of the relevant Celestia-related IBC channel between Celestia and Osmosis can be viewed on 2023-11-01 (channel: CELESTIA / channel-2 - OSMOSIS / channel-6994, source: https://www.mintscan.io/celestia/relayers/channel-2/osmosis/channel-6994, accessed 2026-06-03). The first activity of the relevant Celestia-related IBC channel between Celestia and Injective can be viewed on 2023-11-01 (channel: CELESTIA / channel-7 - INJECTIVE / channel-152, source: https://www.mintscan.io/celestia/relayers/channel-7/injective/channel-152, accessed 2026-06-03).

Celestia is a modular data availability network designed to separate data availability and consensus from execution and settlement. The network orders transactions and makes related data available, while execution and settlement may be performed by rollups or other sovereign chains that use Celestia as a data availability layer. The protocol uses data availability sampling to allow light nodes to verify that block data has been published without downloading full blocks, and Namespaced Merkle Trees to allow applications to identify and verify data relevant to their respective namespaces.

TIA is the native crypto-asset of the Celestia network. It is used to pay fees for publishing data to the network, including PayForBlobs transactions submitted by rollups or other applications. TIA may also be used as a gas token or currency by chains built using the network. The crypto-asset is used in the network's Proof-of-Stake mechanism, where holders may delegate TIA to validators and receive staking rewards. TIA may also be used for protocol governance, including voting on network parameters and matters relating to the community pool.

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

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

DE-HH

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

Celestia Foundation

B.3 Legal form

The legal form of the Celestia Foundation is BSZ8, which corresponds to "Stiftung".

B.4 Registered address

The registered address of Celestia Foundation is c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz,

Liechtenstein,

LI-11

B.5 Head office

The head office address of Celestia Foundation is c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz,

Liechtenstein,

LI-11

B.6 Registration date

The Celestia Foundation was registered on 2022-02-22.

B.7 Legal entity identifier

529900ZZKY6P18UO8C60

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Identity	Function	Business Address
Joon Kim Sang	Director	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein
Batuhan Dasgin	Director	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein
Reinhold Wohlwend	Director	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein
Mustafa Al-Bassam	Director	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein
Ismail Khoffi	Director	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein

B.11 Business activity

The foundation pursues exclusively charitable purposes under Liechtenstein law, namely accelerating technological progress for the benefit of society. It supports and funds the development, promotion and maintenance of decentralised software architectures and protocols, including the Celestia network, together with related research, education and events.

B.12 Parent company business activity

Not applicable.

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

C.1 Name

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

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-asset white paper preparation

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

C.10 Members of the management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

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

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

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

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

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

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Celestia", Short Name: "TIA" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-06-03).

D.2 Crypto-assets name

Long Name: "Celestia" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-06-03).

D.3 Abbreviation

Short Name: "TIA" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-06-03).

D.4 Crypto-asset project description

According to publicly available information (source: https://docs.celestia.org/, accessed 2026-06-03), the Celestia ecosystem is a crypto-asset initiative concerned with the development and operation of a modular data availability network. Celestia is designed to support blockchain-based applications and networks by providing a specialised layer for publishing, ordering and verifying transaction data. Instead of combining execution, settlement, consensus and data availability within one system, Celestia focuses primarily on data availability and consensus.

Within this framework, Celestia allows other blockchain systems to publish their transaction data to the Celestia network so that such data can be made available and verified by network participants. The network uses technical mechanisms intended to allow participants, including light nodes, to check that data has been published without downloading all underlying data themselves. This is intended to support scalability while preserving verifiability for a broader set of users and applications.

The Celestia network operates using a Proof-of-Stake consensus mechanism, under which validators participate in block production and transaction ordering. Participants may delegate TIA to validators in order to support network security and participate indirectly in the consensus process. The TIA crypto-asset functions as the native network-participation and coordination instrument within the Celestia ecosystem.

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

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

Name of person	Type of person	Business address of person	Domicile of company
Joon Kim Sang	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein
Batuhan Dasgin	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein
Reinhold Wohlwend	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein
Mustafa Al-Bassam	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein
Ismail Khoffi	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein
Strange Loop Labs AG	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein
Celestia Foundation	Other person involved in implementation	c/o Revalier Aktiengesellschaft, Pradafant 11, 9490 Vaduz, Liechtenstein	Liechtenstein

D.6 Utility Token Classification

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

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

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

D.8 Plans for the token

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

There is a formally published roadmap for the TIA crypto-asset and the Celestia protocol. Based on the official roadmap and related public communications (sources: https://forum.celestia.org/t/celestia-community-roadmap/1806, https://blog.celestia.org/, https://blog.celestia.org/celestia-vision-2-0-every-market-onchain/; accessed 2026-06-03), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Celestia protocol and the role of the TIA crypto-asset.

Past milestones:

- LazyLedger Whitepaper and Project Foundation (May 2019): The project was founded as LazyLedger, with a whitepaper by Mustafa Al-Bassam published in May 2019.

- Rebrand from LazyLedger to Celestia (15 June 2021): The project announced that LazyLedger would henceforth be rebranded as Celestia.

- Mamaki Public Testnet Launch (25 May 2022): The first public Celestia testnet, Mamaki, was launched.

- Mainnet Beta Launch (31 October 2023): Celestia Mainnet Beta went live, with the genesis block timestamped on 31 October 2023 at 14:00 UTC.

- Lemongrass Upgrade (18 September 2024): The v2 Lemongrass upgrade was activated as the first consensus upgrade since genesis, implementing CIP-17 at a pre-programmed block height.

- First Major Token Unlock (30 October 2024): The first major TIA unlock for initial core contributors and early backers occurred according to the official token documentation.

- Ginger Upgrade (12 December 2024): The v3 Ginger upgrade was activated through in-protocol signalling and reduced the block time from 12 seconds to 6 seconds under CIP-25.

- Lotus Upgrade (28 July 2025): The v4 Lotus upgrade was activated on Mainnet Beta, including CIP-33 and CIP-29. The upgrade reduced the TIA inflation rate from approximately 7.2% to approximately 5.0%.

- Matcha Upgrade (24 November 2025): The v6 Matcha upgrade was activated on Mainnet Beta, including CIP-42 and CIP-41. The upgrade reduced the TIA inflation rate to approximately 2.5%.

- Vision 2.0 Publication (14 January 2026): Celestia published Vision 2.0, describing the "every market onchain" direction and announcing Fibre as a scaling direction for the protocol.

- Private Blockspace Introduction (23 January 2026): Private Blockspace was introduced, with Hibachi identified as the first independent production deployment using verifiable encryption and ZK proofs through Succinct.

- v8 Mainnet Beta Upgrade (5 May 2026): The v8 upgrade was activated on Mainnet Beta under CIP-49. The upgrade carried forward the state-breaking changes initially included in the Hibiscus v7 upgrade, which was not activated on Mainnet Beta. The upgrade introduced adjusted validator commission bounds (CIP-44), a forwarding module for single-signature cross-chain transfers through Hyperlane routes (CIP-45), and a ZK Interchain Security Module for ZK-verified cross-chain messaging (CIP-46).

Future milestones:

- Fibre Scaling Direction (2026 onwards): Celestia Vision 2.0 identifies Fibre as a future scaling direction for the protocol.

- The project aims to become a strategic partner for high-volume market builders and transition blockspace pricing to a sustainable revenue model.

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

D.9 Resource allocation

According to publicly referenced information, in or around March 2021, the project then associated with Celestia is reported to have completed a seed funding round in the amount of approximately USD 1,500,000. Publicly referenced notes identify Interchain Foundation and YZi Labs as investors in this round, while other references describe the investor base more generally as including undisclosed venture capital and angel investors. On that basis, the reported amount and month of the seed financing are treated as publicly referenced, while the precise investor list should be considered not independently verified.

Public sources further indicate that, on or around 19 October 2022, Celestia Labs completed combined Series A and Series B financing rounds in the aggregate amount of approximately USD 55,000,000. The financing was reportedly led by Bain Capital Crypto and Polychain Capital, with participation from Placeholder, Galaxy, Delphi Digital, Blockchain Capital, NFX, Protocol Labs, Figment, Maven 11, Spartan Group and Jump Crypto. Publicly referenced information also identifies Balaji Srinivasan, Eric Wall and Jutta Steiner as participating angel investors.

Public sources further indicate that, on or around 23 September 2024, the Celestia Foundation completed a financing round in the amount of approximately USD 100,000,000. The round is reported to have been led by Bain Capital Crypto, with participation from Syncracy Capital, 1kx, Robot Ventures and Placeholder.

Taken together, the publicly referenced financing amounts described above indicate approximately USD 156,500,000 in reported funding associated with Celestia Labs, the Celestia Foundation, or the broader Celestia project, excluding transactions for which no concrete amount is publicly disclosed. This figure is indicative only and does not account for any undisclosed secondary transactions, undisclosed strategic investments, token allocations, treasury holdings, grants, or non-cash consideration.

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

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

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

There is no fixed maximum supply for the TIA crypto-asset. The total supply of the TIA crypto-asset as of 2026-06-03, corresponding to block height 11,374,656, was approximately 1,170,000,000. This figure represents the total supply at that reference date only and will not remain constant after the date of this white paper. TIA has an inflationary supply model under which new TIA is issued over time to support staking rewards and network security. According to public information, the annual inflation rate was approximately 2.5% as of the v6 upgrade and is expected to decline over time until it reaches a long-term floor of 1.5%.

E.13 Targeted holders

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

E.14 Holder restrictions

Holder restrictions are subject to the rules applicable to the Crypto-Asset Service Provider, as well as to any additional restrictions such provider may impose.

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

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

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

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

F.2 Crypto-asset functionality

According to public information available in the official Celestia documentation (https://docs.celestia.org/, accessed 2026-06-03), TIA is the native crypto-asset of the Celestia network. Celestia is a modular blockchain network designed to provide data availability services for rollups and other blockchain applications. The TIA crypto-asset is used within the Celestia protocol environment and supports several technical and economic functions, including payment of transaction fees, staking, delegation, validator incentives and governance participation.

TIA is used to pay transaction fees on the Celestia network, including fees for PayForBlobs transactions through which users publish data to Celestia's data availability layer. TIA is also used in connection with the proof-of-stake security model of the Celestia network. Validators are required to stake TIA in order to participate in block production and consensus, while other holders may delegate TIA to validators.

The supply of TIA is not subject to a fixed maximum cap. According to the official Celestia documentation, the protocol was launched with an annual inflation rate of 8%, which has subsequently been reduced through protocol upgrades, including CIP-29 and CIP-41. As of the v6 upgrade, the annual inflation rate is approximately 2.5% and is expected to continue declining over time until it reaches the long-term floor of 1.5%.

In addition, TIA is used for governance-related functions within the Celestia ecosystem. TIA holders may participate in governance processes concerning certain network parameters, protocol matters and community pool allocations, subject to the applicable governance framework. Public information also describes the community pool as a mechanism through which a portion of block rewards may support ecosystem-related activities, including development, research and other initiatives connected to the Celestia network.

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

F.3 Planned application of functionalities

Future milestones:

- Fibre Scaling Direction (2026 onwards): Celestia Vision 2.0 identifies Fibre as a future scaling direction for the protocol.

- The project aims to become a strategic partner for high-volume market builders and transition blockspace pricing to a sustainable revenue model

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

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, and is available on the Celestia, Osmosis and Injective networks. The crypto-asset is fungible and divisible up to 6 decimal places. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer any legally enforceable, contractual, shareholder-like, or corporate governance 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: "Celestia" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-06-03).

F.8 Website of the issuer

https://celestia.org/

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

2026-07-08

F.10 Publication date

2026-07-08

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

VTMS6V53Z, 12NRRG38S, TQ1G4JDD1

F.14 Functionally fungible group digital token identifier

M7NN4STH9

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are of a purely technical or operational nature and do not constitute rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments. Accordingly, holders do not acquire any legally enforceable claim against the issuer of the crypto-asset or any third party.

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on the future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-06-03).

G.5 Issuer retained crypto-assets

According to publicly available information on the official Celestia documentation and token allocation disclosures (https://docs.celestia.org and related publicly available token distribution information, accessed on 2026-06-03), a total of 267,900,000 TIA, representing 26.79% of the initial genesis supply of 1,000,000,000 TIA, was allocated to the combined Research & Development and Ecosystem category associated with the Celestia Foundation and core contributors. This allocation was subject to a vesting schedule under which 25% of the allocated TIA became unlocked at the Token Generation Event on 2023-10-31, while the remaining 75% is released linearly between 2024-10-30 and 2027-10-30.

Note: The Research & Development and Ecosystem allocation is publicly disclosed as a combined category and no public information was identified that allocates specific amounts between the Celestia Foundation and individual core contributors. Consequently, the figures presented above should be regarded as the maximum amount potentially attributable to the Celestia Foundation rather than a confirmed Foundation-only holding. Token holdings and transfers remain publicly observable on-chain, but wallet addresses cannot generally be linked to specific natural persons based solely on publicly available information.

G.6 Utility token classification

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

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

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

G.8 Utility tokens redemption

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

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-06-03.

G.13 Supply adjustment mechanisms

Not applicable.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DLT)

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

The following applies to Celestia:

1. Network Protocols

Celestia is a modular Proof-of-Stake blockchain built using the Cosmos SDK and designed to provide consensus and data availability services while leaving execution to external rollups and application-specific layers. Consensus and peer-to-peer networking are provided through CometBFT, a Tendermint-based Byzantine Fault Tolerant consensus engine. Communication between the consensus layer and the application layer is handled through ABCI++, while cross-chain communication may be supported through protocols such as the Inter-Blockchain Communication protocol and other interoperability systems used by connected networks.

2. Transaction and Address Standards

Transactions are processed through Celestia's application layer and include standard account-based transactions as well as PayForBlobs transactions used to publish data to the network. Accounts are associated with addresses, public keys and sequence numbers, and transactions are validated through signature verification, nonce handling, fee deduction and gas accounting. PayForBlobs transactions include blob-related data, namespace information and commitments, allowing data to be published and later referenced by namespace ID, block height and commitment.

3. Blockchain Data Structure & Block Standards

Celestia separates consensus and data availability from execution. The network orders transactions and makes data available, but does not execute general-purpose smart contracts at the base layer. Blob data is arranged into data structures that support data availability sampling, including erasure coding and Namespaced Merkle Trees. Block headers contain cryptographic commitments to the data made available in each block, enabling light nodes and other participants to verify data availability without downloading the full block data.

4. Upgrade & Improvement Standards

Technical changes to Celestia are coordinated through Celestia Improvement Proposals, software releases and the social layer. Core protocol upgrades are not decided solely through token-holder governance in the same manner as many Cosmos SDK-based chains. Since the v2 Lemongrass upgrade, upgrade logic has been agreed through the off-chain CIP and release process, while activation is coordinated through an in-protocol signalling mechanism under which validators run compatible software and signal readiness on chain before activation.

The following applies to Osmosis:

1. Network Protocols

Osmosis is an application-specific Layer 1 blockchain built using the Cosmos SDK. Consensus and peer-to-peer networking are provided through CometBFT, formerly Tendermint Core, which implements Byzantine Fault Tolerant state-machine replication. Osmosis also supports cross-chain communication through the Inter-Blockchain Communication protocol, which enables transfers and messages between IBC-enabled chains.

2. Transaction and Address Standards

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

3. Blockchain Data Structure & Block Standards

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

4. Upgrade & Improvement Standards

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

The following applies to 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.

H.3 Technology used

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

The following applies to Celestia:

1. Decentralised Ledger

Celestia operates as a decentralised ledger that records transactions in an append-only blockchain structure. Blocks are validated and finalised through a Byzantine Fault Tolerant Proof-of-Stake consensus mechanism, with the intention of preserving a transparent record of TIA transfers, staking activity, governance actions and data publication transactions.

2. Private Key Management

To safeguard their TIA holdings, users must securely store their wallet private keys and recovery phrases. The Celestia 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 Cosmos SDK-based networks.

3. Modular Design and Smart Contracting

Celestia follows a modular architecture in which the base layer focuses on consensus and data availability rather than execution. The Celestia base layer does not provide a native general-purpose smart-contract environment. Application logic and execution are expected to take place on external rollups or other connected execution environments that use Celestia for data availability.

The following applies to Osmosis:

1. Decentralised Ledger

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

2. Private Key Management

To safeguard their OSMO holdings, users must securely store their wallet private keys and recovery phrases. The Osmosis protocol does not define standards for private key storage; key management

is handled at the wallet or client level, including software and hardware wallets compatible with the Cosmos SDK.

3. Modular Design and Smart Contracting

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

The following applies to Injective:

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

The platform supports a suite of native modules tailored for DeFi use cases, including decentralised 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, which supports smart contracts across WASM, EVM and SVM. This allows existing DeFi logic to be deployed more easily and supports broader developer adoption.

While this modular design may accelerate innovation and customisation, it also introduces additional complexity and an expanded attack surface compared to monolithic chains.

H.4 Consensus mechanism

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

The following applies to Celestia:

Celestia operates a Proof-of-Stake consensus mechanism based on the Cosmos SDK and CometBFT, a Tendermint-based Byzantine Fault Tolerant consensus engine. CometBFT provides deterministic state-machine replication and is designed to finalise blocks once the required validator voting threshold has been reached.

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

blocks, signing votes and, by signing blocks whose headers commit to the published data, confirming that the data was available to them.

The active validator set is determined by protocol parameters and stake-based selection. Celestia launched with an initial active validator set of 100 validators. Users who do not operate validator infrastructure may participate indirectly by delegating TIA to validators, while remaining exposed to validator-related operational and slashing risks.

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

Celestia's architecture distinguishes consensus from data availability. The network is designed so that light nodes can verify data availability through data availability sampling, rather than relying only on full replication by every participant. Protocol rules, validator participation and network parameters are implemented through the Celestia software, with a defined subset of parameters modifiable through on-chain governance and other parameters requiring software-level changes.

The following applies to Osmosis:

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

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

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

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

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

The following applies to 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 behaviour. The system may be exposed to validator collusion or governance capture.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

The following applies to Celestia:

Validator and Delegator Rewards

Validators earn rewards for participating in consensus, producing blocks and supporting the operation of the network. Delegators who stake their TIA with validators receive a proportional share of validator rewards after validator commission. Rewards are funded through protocol-defined token issuance and collected transaction fees. A portion of block rewards is allocated to the community pool, which may be used for ecosystem-related purposes through governance processes.

Token Issuance

TIA issuance follows a protocol-defined inflation model intended to reward validators and delegators for securing the network. Publicly communicated protocol changes have reduced the inflation rate over time, while the long-term issuance model is intended to move towards a lower continuing inflation rate. The issuance schedule is fixed in the protocol software and is not modifiable through on-chain governance; changes require a consensus-breaking protocol upgrade.

Transaction Fees

Users pay transaction fees in TIA for network activity, including transfers, staking-related transactions, governance actions and PayForBlobs transactions used to publish data to Celestia. Fees are calculated using gas limits and gas prices. For blob transactions, the fee amount may depend in part on the size of the data being published. Transaction fees are deducted by the state machine and distributed through the protocol's fee collection and distribution mechanism to validators and, after validator commission, their delegators.

Slashing and Penalties

Celestia uses a bonded Proof-of-Stake model in which validator participation is supported by economic collateral. Validators and delegators may be exposed to penalties if validator conduct breaches applicable protocol rules. Public technical materials also describe data availability-related

penalty mechanisms as part of the intended security model, although certain specific slashing mechanisms may depend on implementation status and protocol upgrades. Delegators are exposed to the risks associated with the validators to whom they delegate.

The following applies to Osmosis:

Validator and Delegator Rewards

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

Liquidity Provider Incentives

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

Transaction Fees

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

Slashing and Penalties

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

The following applies to Injective:

The network incentivises liquidity providers and validators through block rewards and transaction fees paid in INJ. Liquidity mining programmes and governance-driven reward distribution may influence participation but can also result in centralisation of liquidity or speculative behaviour. 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

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

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

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

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

5. Operational and information risks

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

information asymmetry and place less informed investors at a disadvantage when making trading decisions.

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Protocol and software vulnerability risk

The protocol rules, client software implementations, execution and consensus layer components, or related technical elements that define the crypto-asset's parameters or govern its transfers may contain coding errors or security vulnerabilities. Exploitation of such weaknesses can result in unintended consequences, including loss of funds or disruption of network functionality.

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the crypto-asset

Celestia

S.4 Consensus Mechanism

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

The following applies to Celestia:

Celestia operates a Proof-of-Stake consensus mechanism based on the Cosmos SDK and CometBFT, a Tendermint-based Byzantine Fault Tolerant consensus engine. CometBFT provides deterministic state-machine replication and is designed to finalise blocks once the required validator voting threshold has been reached.

Consensus participants are validators who bond TIA, or receive delegated TIA from third-party holders. Validator voting power is determined by the amount of TIA bonded to the validator, including delegated stake. Validators participate in block production and consensus by proposing blocks, signing votes and, by signing blocks whose headers commit to the published data, confirming that the data was available to them.

The active validator set is determined by protocol parameters and stake-based selection. Celestia launched with an initial active validator set of 100 validators. Users who do not operate validator infrastructure may participate indirectly by delegating TIA to validators, while remaining exposed to validator-related operational and slashing risks.

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

Celestia's architecture distinguishes consensus from data availability. The network is designed so that light nodes can verify data availability through data availability sampling, rather than relying only on full replication by every participant. Protocol rules, validator participation and network parameters are implemented through the Celestia software, with a defined subset of parameters modifiable through on-chain governance and other parameters requiring software-level changes.

The following applies to Osmosis:

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

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

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

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

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

The following applies to 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 behaviour. The system may be exposed to validator collusion or governance capture.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is native to the Celestia blockchain and is also available on the Osmosis and Injective networks in accordance with the standards described below.

The following applies to Celestia:

Validator and Delegator Rewards

Validators earn rewards for participating in consensus, producing blocks and supporting the operation of the network. Delegators who stake their TIA with validators receive a proportional share of validator rewards after validator commission. Rewards are funded through protocol-defined token issuance and collected transaction fees. A portion of block rewards is allocated to the community pool, which may be used for ecosystem-related purposes through governance processes.

Token Issuance

TIA issuance follows a protocol-defined inflation model intended to reward validators and delegators for securing the network. Publicly communicated protocol changes have reduced the inflation rate over time, while the long-term issuance model is intended to move towards a lower continuing inflation rate. The issuance schedule is fixed in the protocol software and is not modifiable through on-chain governance; changes require a consensus-breaking protocol upgrade.

Transaction Fees

Users pay transaction fees in TIA for network activity, including transfers, staking-related transactions, governance actions and PayForBlobs transactions used to publish data to Celestia. Fees are calculated using gas limits and gas prices. For blob transactions, the fee amount may depend in part on the size of the data being published. Transaction fees are deducted by the state machine and distributed through the protocol's fee collection and distribution mechanism to validators and, after validator commission, their delegators.

Slashing and Penalties

Celestia uses a bonded Proof-of-Stake model in which validator participation is supported by economic collateral. Validators and delegators may be exposed to penalties if validator conduct breaches applicable protocol rules. Public technical materials also describe data availability-related penalty mechanisms as part of the intended security model, although certain specific slashing mechanisms may depend on implementation status and protocol upgrades. Delegators are exposed to the risks associated with the validators to whom they delegate.

The following applies to Osmosis:

Validator and Delegator Rewards

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

rewards. The allocation of newly issued tokens is subject to protocol governance and may be adjusted over time.

Liquidity Provider Incentives

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

Transaction Fees

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

Slashing and Penalties

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

The following applies to Injective:

The network incentivises liquidity providers and validators through block rewards and transaction fees paid in INJ. Liquidity mining programmes and governance-driven reward distribution may influence participation but can also result in centralisation of liquidity or speculative behaviour. 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

2025-06-05

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

2026-06-05

S.8 Energy consumption

80791.97748 kWh/a

S.9 Energy consumption sources and methodologies

For the calculation of energy consumption, the so-called "bottom-up" approach is used. Nodes are considered the central factor for the energy consumption of the underlying network. The relevant assumptions are based on empirical findings obtained through 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 relevant client software. The energy consumption of the relevant hardware devices was measured in certified test laboratories. Where available, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used to determine all technically equivalent implementations of the crypto-asset in scope, and the relevant mappings are updated regularly based on data from the Digital Token Identifier Foundation.

Information regarding the hardware used and the number of participants in the network is based on assumptions that are verified on a best-effort basis using empirical data. In general, participants are assumed to act largely economically rationally. In line with the precautionary principle, conservative assumptions are made where uncertainty exists, meaning that estimates tend towards the higher end of the reasonably plausible 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).

S.10 Renewable energy consumption

32.2548716093 %

S.11 Energy intensity

0.00012 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

26.88863 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 determined using public information sites, open-source and in-house-developed crawlers. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal energy consumption with respect to one additional transaction.

Ember (2025); Energy Institute, Statistical Review of World Energy (2024), with major processing by Our World in Data. “Share of electricity generated by renewables - Ember and Energy Institute” [dataset]. Underlying sources: Ember, “Yearly Electricity Data Europe”; Ember, “Yearly

Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: https://ourworldindata.org/grapher/share-electricity-renewables

S.16 Key GHG sources and methodologies

To determine GHG emissions, the locations of the nodes are determined using public information sites, open-source crawlers, and crawlers developed in-house. Where no information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal emission intensity with respect to one additional transaction.

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.