CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

# White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG KCHF60NW7

# Preamble

## 00. Table of Content

## 01. Date of notification

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

## 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 Compound (COMP) referred to in this white paper is a crypto-asset other than EMTs and ARTs, and is issued on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks as of 2026-01-22. The maximum supply of the crypto-asset is fixed at 10,000,000 units. The first activity on Ethereum can be viewed on 2020-03-04 (transaction hash: 0xe87715364f1733c893b4dca5c8e932627e5ddcc2076f8fc69a9d38c5563c4ed1, source: https://etherscan.io/tx/0xe87715364f1733c893b4dca5c8e932627e5ddcc2076f8fc69a9d38c5563c4ed1, accessed 2026-01-22). The first activity on Binance Smart Chain can be viewed on 2020-09-30 (transaction hash: 0x113e1973e956c3f5d7dedaf45fd5338dc39424f21e14eeaf767ceb2882f759a1, source: https://bscscan.com/tx/0x113e1973e956c3f5d7dedaf45fd5338dc39424f21e14eeaf767ceb2882f759a1, accessed 2026-01-22). The first activity on Avalanche C-Chain can be viewed on 2021-07-23 (transaction hash: 0xb943c180150a8c2df75ef5cd0f4169485d409a1d9beee7390d7ea99aaa4700aa, source: https://snowtrace.io/tx/0xb943c180150a8c2df75ef5cd0f4169485d409a1d9beee7390d7ea99aaa4700aa, accessed 2026-01-22). The first activity on Gnosis can be viewed on 2020-08-24 (transaction hash: 0x83e17450ebb600cee26b5ea7336af84c20820d6c178e3d16532a967af0fbbaab, source: https://gnosisscan.io/tx/0x83e17450ebb600cee26b5ea7336af84c20820d6c178e3d16532a967af0fbbaab, accessed 2026-01-22). The first activity on Near Protocol can be viewed on 2021-09-16 (transaction hash: B3L5cAFgKrwW6oLgU8a4juiB5n3CZfJtckFxgytXVGn8, source: https://nearblocks.io/txns/B3L5cAFgKrwW6oLgU8a4juiB5n3CZfJtckFxgytXVGn8, accessed 2026-01-22). The first activity on Solana can be viewed on 2021-10-14 (transaction hash: b1kRpgg1pg35A6e43NSRjm51vXuQ5uR2Tkyvny5NhPoD7AkjoBsW4DXLW6KyHq5Wo5gMQUcVQAcTPL7MU4qHwE
source: https://solscan.io/tx/b1kRpgg1pg35A6e43NSRjm51vXuQ5uR2Tkyvny5NhPoD7AkjoBsW4DXLW6KyHq5Wo5gMQUcVQAcTPL7MU4qHwE
accessed 2026-01-22).

Compound Finance is a decentralised, open-source protocol deployed primarily on the Ethereum blockchain that facilitates algorithmic money markets for crypto-assets through non-custodial smart contracts. The protocol enables participants to supply supported crypto-assets to shared liquidity pools and to borrow crypto-assets against over-collateralised positions, with interest rates determined automatically based on asset-specific utilisation metrics. Protocol interactions follow a user-to-protocol model rather than bilateral peer-to-peer agreements, with all balances, collateral requirements, liquidations, and interest accruals enforced programmatically by smart contracts.

Within this technical framework, the COMP crypto-asset functions as the governance instrument of the Compound protocol. COMP may be used to submit, vote on, or delegate voting power for governance proposals that affect protocol parameters, supported assets, risk configurations, and reserve management mechanisms. Governance participation is conducted entirely on-chain and is subject to predefined proposal thresholds, voting periods, and execution delays. The protocol has undergone multiple architectural iterations, including earlier pooled-asset markets and the later single-base-asset market design (Compound III), which is intended to reduce systemic risk and simplify collateral and liquidation mechanics.

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

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

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

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

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

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

### A.1 Name

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

### A.2 Legal form

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

### A.3 Registered address

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

Germany,

federal state Hamburg.

### A.4 Head office

Crypto Risk Metrics GmbH has no head office.

### A.5 Registration date

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

### A.6 Legal entity identifier

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

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

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

### A.8 Contact telephone number

+4915144974120

### A.9 E-mail address

info@crypto-risk-metrics.com

### A.10 Response time (Days)

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

### A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

### A.12 Members of the management body

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

### A.13 Business activity

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

### A.14 Parent company business activity

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

### A.15 Newly established

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

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

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

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

2024 (unaudited): negative EUR 50.891,81

2023 (unaudited): negative EUR 27.665,32

2022: EUR 104.283,00.

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

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

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

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

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

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

## A.17 Financial condition since registration

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

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

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

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

### B.2 Name

The token does not appear to be issued by a formal company or foundation in the traditional sense. Instead, it follows a decentralized approach.

### B.3 Legal form

Not applicable.

### B.4 Registered address

Not applicable.

Not applicable.

Not applicable.

### B.5 Head office

Not applicable.

Not applicable.

Not applicable.

### B.6 Registration date

The token does not appear to be issued by a formal company or foundation in the traditional sense. Instead, it follows a decentralized approach.

### B.7 Legal entity identifier

Not applicable, as the project follows a decentralized approach.

### 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 |
|---|---|---|
| Not applicable | Not applicable | Not applicable |

### B.11 Business activity

Not applicable.

### 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: "Compound", Short Name: "COMP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-01-22).

### D.2 Crypto-assets name

Long Name: "Compound" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-01-22).

### D.3 Abbreviation

Short Name: "COMP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-01-22).

### D.4 Crypto-asset project description

According to publicly available information (source: https://docs.compound.finance/, accessed on 2026-01-22), Compound Finance is a decentralised crypto-asset project concerned with the development and operation of an Ethereum-based money-market protocol. The project is designed to facilitate the algorithmic lending and borrowing of crypto-assets through smart contracts, without reliance on traditional financial intermediaries. Users interact directly with the protocol in a user-to-protocol model, whereby supplied assets are aggregated into fungible liquidity pools and made available for borrowing against overcollateralised positions.

Within this technical framework, the Compound protocol enables users to supply supported crypto-assets in order to earn variable interest rates, and to borrow assets by providing other crypto-assets as collateral. Interest rates are determined algorithmically based on predefined utilisation-rate models reflecting supply and demand dynamics for each supported asset. The protocol incorporates automated risk-management mechanisms, including liquidation processes that may be triggered if collateral values fall below specified thresholds. These processes are executed entirely on-chain and are dependent on the correct functioning, security, and continued availability of the underlying smart-contract infrastructure and the Ethereum network.

The protocol has undergone multiple iterations since its initial deployment. Earlier versions introduced tokenised representations of supplied assets (cTokens), which accrue value over time as interest is earned. Subsequent versions, including Compound III (also referred to as “Comet”), introduced architectural changes such as a single-base-asset borrowing model intended to improve capital efficiency and reduce systemic risk. The scope, configuration, and availability of supported assets, risk parameters, and protocol features are subject to change through governance decisions and technical updates.

The COMP crypto-asset functions as an element within this broader technical and governance framework. COMP is an ERC-20 crypto-asset intended primarily to facilitate decentralised governance of the Compound protocol. Holders of COMP may propose and vote on governance actions affecting protocol parameters, including the addition or removal of supported assets, adjustments to interest-rate models, collateral factors, and other risk-management settings. Voting rights may be exercised directly or delegated to other addresses. In addition, COMP has been distributed as an incentive mechanism to encourage participation in the protocol by suppliers and borrowers. COMP is not used to pay network transaction fees, which are paid in ETH on the Ethereum network.

The introduction and distribution of COMP were designed as part of a progressive decentralisation process, transitioning administrative control of the protocol from its original development team to a community-governed system. COMP was not issued as part of a public fundraising event but was allocated through predefined distribution mechanisms, including protocol usage rewards, community-controlled reserves, educational distributions, and allocations to founders, team members, and early stakeholders subject to time-based vesting conditions. The actual influence and effectiveness of governance processes depend on participation levels, delegation practices, and the broader economic and technical environment in which the protocol operates.

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

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

| Type of person | Name of person | Business address of person | Domicile of company |
|---|---|---|---|
| Other person involved in implementation | Compound Labs, Inc. (San Francisco Branch) | 1420 36th Ave, San Francisco, CA, 94122, United States | United States |

### D.6 Utility Token Classification

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

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

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

## D.8 Plans for the token

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

There is no formally published multi-year roadmap for the COMP crypto-asset. Based on public information (https://compound.finance/ and https://medium.com/compound-finance, accessed 2026-01-22), several protocol upgrades, ecosystem initiatives, and token-related developments have been communicated that affect the evolution of the Compound interoperability infrastructure and the role of the COMP token.

Past milestones:

- Initial Protocol Launch (September 2018): The first version of the Compound protocol was deployed on the Ethereum mainnet, enabling algorithmic money market functionality.

- Compound v2 Upgrade (May 2019): A major protocol upgrade introduced cTokens as transferable representations of supplied assets and marked the beginning of progressive decentralisation.

- Governance Handover to Token Holders (16-04-2020): Administrative control over protocol parameters and upgrades was formally transferred from the founding team to community governance mediated through the COMP crypto-asset.

- Commencement of COMP Distribution (June 2020): Distribution of the COMP crypto-asset to protocol participants began, enabling decentralised governance participation by users.

- Compound III ("Comet") Launch (26-08-2022): A new protocol version was introduced with a single-base-asset design, modifying lending and borrowing mechanics.

- Conclusion of Token Release Schedule (June 2024): The predefined multi-year release schedule for COMP allocations to founders, team members, and investors was completed.

Future milestones:

- Governance-Driven Protocol Adjustments (No fixed date): Future changes to supported assets, risk parameters, and protocol configurations may be proposed and implemented through COMP-based governance processes.

- Immunefi Bug Bounty Program Renewal (19-01-2026, proposed): A proposal was submitted to renew the managed bug bounty partnership with Immunefi for a further one-year period, aiming to support the planned Compound V4 mainnet launch through continued expert triage, audit competition support, automated code review services, and emergency response mechanisms, subject to governance approval and implementation.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past performance or implementation does not guarantee future success, and changes may materially affect the value or utility of the COMP token for holders.

### D.9 Resource allocation

Based on information from various third-party and industry sources, it is reported that Compound Finance (Compound Labs, Inc.) has raised external financing through multiple private funding rounds conducted between approximately May 2018 and March 2025. According to these sources, the project is reported to have raised approximately USD 71.9 million in aggregate, primarily from venture capital firms and strategic investors active in the digital assets and financial technology sectors.

Publicly available information indicates that an initial seed funding round in or around May 2018 reportedly raised approximately USD 8.2 million, with participation from venture capital firms including Andreessen Horowitz, Bain Capital Ventures, and Polychain Capital, among others.

Subsequently, a Series A financing round in or around November 2019 is reported to have raised approximately USD 25 million, with Andreessen Horowitz referenced as lead investor. In addition, public sources refer to further financing activity, including a round in early 2020 for which no public details on the amount or participating investors are disclosed, as well as debt financing reported in or around November 2022 amounting to approximately USD 37.6 million. A further minor funding event in March 2025, reportedly amounting to approximately USD 95,000, is also referenced in public databases, without disclosure of investor identities.

Across these reported funding events, publicly named or referenced investors include venture capital and strategic investment firms such as Andreessen Horowitz, Bain Capital Ventures, Polychain Capital, Coinbase, Transmedia Capital, Compound Ventures, Abstract Ventures, Danhua Capital, NodeRise Capital, and Davoa Capital.

However, all of the above information is derived exclusively from public announcements, third-party databases, and industry publications. The issuer or project has not independently confirmed the existence, timing, amount, valuation, legal structure, or contractual terms of these financing rounds. As a result, the reported funding amounts, investor participation, and aggregate capital raised cannot be independently verified and should therefore be considered indicative only, rather than definitive or exhaustive.

### D.10 Planned use of Collected funds or crypto-Assets

Not applicable, as this white paper was drawn up for the admission to trading and not for collecting funds for the crypto-asset-project.

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

### E.1 Public offering or admission to trading

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

### E.2 Reasons for public offer or admission to trading

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

### E.3 Fundraising target

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

### E.4 Minimum subscription goals

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

### E.5 Maximum subscription goals

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

### E.6 Oversubscription acceptance

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

### E.7 Oversubscription allocation

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

### E.8 Issue price

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

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

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

### E.10 Subscription fee

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

### E.11 Offer price determination method

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

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

The maximum supply of the crypto-asset is set at 10,000,000 units. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

### E.13 Targeted holders

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

### E.14 Holder restrictions

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

### E.15 Reimbursement notice

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

### E.16 Refund mechanism

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

### E.17 Refund timeline

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

### E.18 Offer phases

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

### E.19 Early purchase discount

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

### E.20 Time-limited offer

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

### E.21 Subscription period beginning

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

### E.22 Subscription period end

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

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

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

### E.24 Payment methods for crypto-asset purchase

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

### E.25 Value transfer methods for reimbursement

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

### E.26 Right of withdrawal

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

### E.27 Transfer of purchased crypto-assets

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

### E.28 Transfer time schedule

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

### E.29 Purchaser's technical requirements

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

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

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

### E.31 CASP identifier

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

### E.32 Placement form

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

### E.33 Trading platforms name

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

### E.34 Trading platforms Market identifier code (MIC)

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

### E.35 Trading platforms access

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

### E.36 Involved costs

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

### E.37 Offer expenses

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

### E.38 Conflicts of interest

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

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

### E.39 Applicable law

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

### E.40 Competent court

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

## Part F – Information about the crypto-assets

### F.1 Crypto-asset type

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

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

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

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

### F.2 Crypto-asset functionality

The COMP token does not confer ownership, profit participation, governance rights over the issuer or any related entity, or any form of economic entitlement. All functionalities are technical in nature and relate exclusively to interactions within the Compound protocol environment. The actual usability of COMP depend on factors such as smart-contract performance, governance outcomes, network conditions, and the continued operation of the underlying blockchain infrastructures, including Ethereum and compatible execution environments, which are outside the control of token holders.

### F.3 Planned application of functionalities

Future milestones:

- Governance-Driven Protocol Adjustments (No fixed date): Future changes to supported assets, risk parameters, and protocol configurations may be proposed and implemented through COMP-based governance processes.

- Immunefi Bug Bounty Program Renewal (19-01-2026, proposed): A proposal was submitted to renew the managed bug bounty partnership with Immunefi for a further one-year period, aiming to support the planned Compound V4 mainnet launch through continued expert triage, audit competition support, automated code review services, and emergency response mechanisms, subject to governance approval and implementation.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past performance or implementation does not guarantee future success, and changes may materially affect the value or utility of the COMP token for holders.

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

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

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

### F.5 The type of submission

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

### F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs and is available on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol, and Solana networks. It is fungible up to 18 decimal places on Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, and Near Protocol, and up to 8 decimal places on Solana. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics such as supply, demand, and liquidity in secondary markets.

### F.7 Commercial name or trading name

Long Name: "Compound" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-01-22).

### F.8 Website of the issuer

As no issuer is identified for the crypto-asset, there is no website of an issuer within the meaning of Regulation (EU) 2023/1114 (MiCAR).

General, non-issuer-related information about the underlying project is made publicly available at: https://compound.finance/.

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

2026-03-03

### F.10 Publication date

2026-03-03

### 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

NVQLHF357, DXNJVNZC9, FK0F23L2H, QHFMLBRMD, BKJMCZ016, R263M88WC

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

KCHF60NW7

### F.15 Voluntary data flag

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

### F.16 Personal data flag

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

### F.17 LEI eligibility

LEI eligibility cannot be assessed, as the issuer cannot be identified as a legal person.

### F.18 Home Member State

Germany

### F.19 Host Member States

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

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

## G.1 Purchaser rights and obligations

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

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

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

## G.2 Exercise of rights and obligations

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

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

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

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

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

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

## G.4 Future public offers

Information on the future offers to the public of crypto-assets were not available at the time of writing this white paper (2026-01-22).

## G.5 Issuer retained crypto-assets

The token does not appear to be issued by a formal company or foundation in the traditional sense. Instead, it follows a decentralized approach.

At the time of the protocol's decentralisation, the fixed maximum supply of 10,000,000 COMP was historically allocated across the following stakeholder categories:

- Protocol users: approximately 42%

- Founders and core team: approximately 26%

- Early investors and shareholders: approximately 24%

- Community and governance initiatives: approximately 8%

Note: While wallet-level token balances can be verified on-chain, allocations to specific persons or entities cannot be independently confirmed, as public blockchain addresses cannot be reliably attributed to identifiable natural or legal persons. Consequently, the precise economic influence of individual stakeholders cannot be determined. Token movements, changes in ownership, or internal re-allocations may occur without prior notice and could affect governance dynamics, market perceptions, or anticipated economic outcomes.

### 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 2026-01-22.

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

### G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 10,000,000 units according to public information (Source: https://docs.compound.finance/, accessed 2026-01-22). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

### G.14 Token value protection schemes

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

### G.15 Token value protection schemes description

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

### G.16 Compensation schemes

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

### G.17 Compensation schemes description

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

### G.18 Applicable law

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

### G.19 Competent court

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

## Part H – information on the underlying technology

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

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

### H.2 Protocols and technical standards

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

The following applies to Ethereum:

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

1. Network Protocols

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

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

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

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

2. Transaction and Address Standards

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

Transaction Types:

- Legacy Transactions (pre-EIP-1559)

- Type 0 (Pre-EIP-1559 transactions)

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

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

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

3. Blockchain Data Structure & Block Standards

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

Each block contains:

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

- Transactions: Smart contract executions and token transfers.

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

4. Upgrade & Improvement Standards

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

The following applies to Binance Smart Chain:

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

The following applies to Avalanche C-Chain:

Avalanche supports the Ethereum Virtual Machine on its C-Chain and implements standard token protocols such as ERC-20 and ERC-721 for compatibility. Its architecture also allows custom virtual machines via the Subnet framework.

The following applies to Gnosis:

Gnosis is built on the Ethereum Virtual Machine (EVM) standard and supports standards like ERC-20 and ERC-721 token protocols. Smart contracts follow widely adopted Ethereum standards, ensuring interoperability with existing tools and dApps

The following applies to Near Protocol:

1. Network and communication protocols

NEAR is a sharded Layer-1 blockchain that uses a peer-to-peer network to distribute blocks, transaction data and state updates.

- The protocol uses the Nightshade sharding design, where multiple shards process state in parallel but jointly produce a single logical block per block height.

- Interactions between accounts and shards are handled through receipt-based asynchronous message passing, which allows cross-shard transactions without synchronous locking.

- Validators and block producers exchange block headers, chunks and receipts through NEAR’s native peer-to-peer networking layer.

2. Account and addressing standards

NEAR uses a flexible, human-readable account system instead of fixed-length cryptographic addresses.

- Named accounts such as alice.near or dao.project.near act like domain names and can create hierarchical sub-accounts.

- Implicit accounts are 64-character hexadecimal addresses derived directly from a public key.

- Ethereum-style 0x addresses are also supported, allowing compatibility with Ethereum wallets such as MetaMask.

3. Access key and permission model

NEAR accounts can contain multiple cryptographic keys with different permissions.

- Full-access keys allow complete control of an account, including transfers, contract deployment and key management.

- Function-call keys are restricted and can only call specific smart-contract methods and cannot transfer NEAR or modify ownership.

This allows fine-grained security and enables wallet delegation and application-specific permissions.

4. Cryptographic and security standards

NEAR uses standard cryptographic primitives to secure accounts, transactions and validator assignments.

- Ed25519 is used for public-private key pairs and transaction signatures.

- A Verifiable Random Function (VRF) is used to assign validators to shards in an unpredictable way, reducing the risk of targeted attacks.

- Erasure-coded data distribution ensures that block data can be reconstructed even if some producers are offline or malicious.

5. Transaction, asset and data standards

- The native NEAR token is used for transaction fees, storage deposits and protocol-level accounting.

- NEAR Enhancement Proposals (NEPs) define protocol-level standards.

- NEP-366 enables meta-transactions via DelegateActions, allowing third parties to pay transaction fees on behalf of users.

- NEP-536 defines how unused gas is refunded to improve execution efficiency.

- Blockchain data, transactions and contract state are serialized using Borsh, a compact and deterministic binary format optimized for hashing and storage.

6. Storage and state accounting

NEAR applies a storage staking model.

- Accounts must lock NEAR tokens proportional to the amount of on-chain data they store, at a rate of approximately 1 NEAR per 100 kB.

- This ensures that long-term state storage is paid for by the parties that consume it.

7. Smart-contract execution

Smart contracts are executed in a deterministic runtime.

- Contracts run as WebAssembly (WASM) bytecode.

- Contract calls and cross-contract interactions are executed through receipt-based message passing.

- Execution results are deterministic so that all nodes reach the same outcome.

The following applies to Solana:

The tokens were created with Solana’s Token Program, a smart contract that is part of the Solana Program Library (SPL). Such tokens are commonly referred to as SPL-token. The token itself is not an additional smart contract, but what is called a data account on Solana. As the name suggests data accounts store data on the blockchain. However, unlike smart contracts, they cannot be executed and cannot perform any operations. Since one cannot interact with data accounts directly, any interaction with an SPL-token is done via Solana’s Token Program. The source code of this smart contract can be found here https://github.com/solana-program/token.

The Token Program is developed in Rust, a memory-safe, high-performance programming language designed for secure and efficient development. On Solana, Rust is said to be the primary language used for developing on-chain programs (smart contracts), intended to ensure safety and reliability in decentralized applications (dApps).

Core functions of the Token Program:

initialize_mint() → Create a new type of token, called a mint

mint_to() → Mints new tokens of a specific type to a specified account

burn() → Burns tokens from a specified account, reducing total supply

transfer() → Transfers tokens between accounts

approve() → Approves a delegate to spend tokens on behalf of the owner

set_authority() → Updates authorities (mint, freeze, or transfer authority)

These functions ensure basic operations like transfers, and minting/burning can be performed within the Solana ecosystem.

In addition to the Token Program, another smart contract, the Metaplex Token Metadata Program is commonly used to store name, symbol, and URI information for better ecosystem compatibility. This additional metadata has no effect on the token's functionality.

## H.3 Technology used

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

The following applies to Ethereum:

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

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

3. Cryptographic Integrity: Ethereum employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers. The Keccak-256 (SHA-3 variant) Hashing Algorithm is used for hashing and address generation. The crypto-asset uses

ECDSA with secp256k1 curve for key generation and digital signatures. Next to that, BLS (Boneh-Lynn-Shacham) signatures are used for validator aggregation in PoS.

The following applies to Binance Smart Chain:

1. BSC-Compatible Wallets

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

2. Ledger

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

3. BEP-20 Token Standard

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

4. Scalability and Transaction Efficiency

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

The following applies to Avalanche C-Chain:

Avalanche features a modular, multi-chain design enabling the creation of custom subnets, each with its own blockchain and rules, while intending to maintain high throughput and low latency.

The following applies to Gnosis:

Gnosis uses an Ethereum-compatible architecture focused on efficient governance and DAO applications. By employing Rollups and an energy-efficient infrastructure, scalability and transaction performance are enhanced.

The following applies to Near Protocol:

1. Decentralized ledger

- The NEAR blockchain acts as a decentralized ledger that records all NEAR token transfers and smart-contract interactions.

2. Smart-contract execution environment

- NEAR uses a runtime layer based on WebAssembly (WASM) to execute smart contracts.

- Smart contracts run in an isolated and deterministic environment, ensuring that all network participants compute the same result from the same inputs.

3. Token and application standards

- The NEAR ecosystem supports native fungible tokens (FTs) and non-fungible tokens (NFTs) defined through NEAR Enhancement Proposals (NEPs).

- NEP-366 enables meta-transactions, allowing transactions to be submitted on behalf of users by third-party relayers, supporting gas-sponsored interactions and easier onboarding.

The following applies to Solana:

1. Solana-Compatible Wallets: The tokens are supported by all wallets compatible with Solana’s Token Program

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

3. SPL Token Program: The SPL (Solana Program Library) Token Program is an inherent Solana smart contract built to create and manage new types of tokens (so called mints). This is significantly different from ERC-20 on Ethereum, because a single smart contract that is part of Solana’s core functionality and as such is open source, is responsible for all the tokens. This ensures a high uniformity across tokens at the cost of flexibility.

4. Blockchain Scalability: With its intended capacity for processing a lot of transactions per second and in most cases low fees, Solana is intended to enable efficient token transactions, maintaining high performance even during peak network usage.

Security Protocols for Asset Custody and Transactions:

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

2. Cryptographic Integrity: Solana employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers.

## H.4 Consensus mechanism

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

Core Components

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

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

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

Consensus Process

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

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

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

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

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

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

The following applies to Avalanche C-Chain:

The Avalanche blockchain network employs a unique Proof-of-Stake consensus mechanism called Avalanche Consensus, which involves three interconnected protocols: Snowball, Snowflake, and Avalanche.

Avalanche Consensus Process:

1. Snowball Protocol:

- Random Sampling: Each validator randomly samples a small, constant-sized subset of other validators.

- Repeated Polling: Validators repeatedly poll the sampled validators to determine the preferred transaction.

- Confidence Counters: Validators maintain confidence counters for each transaction, incrementing them each time a sampled validator supports their preferred transaction.

- Decision Threshold: Once the confidence counter exceeds a pre-defined threshold, the transaction is considered accepted.

2. Snowflake Protocol:

- Binary Decision: Enhances the Snowball protocol by incorporating a binary decision process. Validators decide between two conflicting transactions.

- Binary Confidence: Confidence counters are used to track the preferred binary decision.

- Finality: When a binary decision reaches a certain confidence level, it becomes final.

3. Avalanche Protocol:

- DAG Structure: Uses a Directed Acyclic Graph (DAG) structure to organize transactions, allowing for parallel processing and higher throughput.

- Transaction Ordering: Transactions are added to the DAG based on their dependencies, ensuring a consistent order.

- Consensus on DAG: While most Proof-of-Stake Protocols use a Byzantine Fault Tolerant (BFT) consensus, Avalanche uses the Avalanche Consensus, Validators reach consensus on the structure and contents of the DAG through repeated Snowball and Snowflake.

The following applies to Gnosis:

Gnosis operates with a Proof-of-Stake (PoS) consensus mechanism, where validators secure the network by staking GNO tokens and participating in block production.

The following applies to Near Protocol:

1. Core consensus model

- NEAR does not use miners; instead, it relies on validators that stake NEAR tokens to participate in block and chunk production.

- Nightshade is a sharded consensus model in which all shards jointly produce a single logical block for each block height.

- Each shard produces a chunk containing transactions and state changes for that shard, and a designated block producer aggregates all chunks into one block.

2. Validator roles

- Block and Chunk Producers are responsible for creating blocks and producing shard chunks.

- Chunk Validators verify the correctness of chunks produced by other validators.

- Hidden Validators are randomly assigned to shards using a Verifiable Random Function (VRF) and verify chunk correctness without their assignment being known in advance.

- Fishermen are observing nodes that monitor the network and can submit fraud proofs if invalid behavior is detected.

3. Block production and finality

- Blocks and chunks are produced at an interval of approximately one second.

- Transactions become final once all related receipts (cross-shard execution messages) have been processed.

- Most transactions reach finality within 1 to 3 seconds, depending on cross-shard execution.

The following applies to Solana:

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

Core Concepts

1. Proof of History (PoH):

Time-Stamped Transactions: PoH is a cryptographic technique that timestamps transactions, intended to creating a historical record that proves that an event has occurred at a specific moment in time.

Verifiable Delay Function: PoH uses a Verifiable Delay Function (VDF) to generate a unique hash that includes the transaction and the time it was processed. This sequence of hashes provides a verifiable order of events, intended to enabling the network to efficiently agree on the sequence of transactions.

2. Proof of Stake (PoS):

Validator Selection: Validators are chosen to produce new blocks based on the number of SOL tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

cryptographic clock for the network.

3. Block Production:

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

4. Consensus and Finalization:

Other validators verify the block produced by the leader validator. They check the correctness of the PoH sequence and validate the transactions within the block. Once the block is verified, it is added to the blockchain. Validators sign off on the block, and it is considered finalized.

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

Staking: Validators must stake SOL tokens to participate in the consensus process. This staking acts as collateral, incentivizing validators to act honestly. If a validator behaves maliciously or fails to perform, they risk losing their staked tokens.

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

3. Economic Penalties:

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

### H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

Incentive Mechanisms

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

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

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

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

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

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

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

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

The following applies to Avalanche C-Chain:

Avalanche uses a consensus mechanism known as Avalanche Consensus, which relies on a combination of validators, staking, and a novel approach to consensus to ensure the network's security and integrity.

1. Validators:

- Staking: Validators on the Avalanche network are required to stake AVAX tokens. The amount staked influences their probability of being selected to propose or validate new blocks.

- Rewards: Validators earn rewards for their participation in the consensus process. These rewards are proportional to the amount of AVAX staked and their uptime and performance in validating transactions.

- Delegation: Validators can also accept delegations from other token holders. Delegators share in the rewards based on the amount they delegate, which incentivizes smaller holders to participate indirectly in securing the network.

2. Economic Incentives:

- Block Rewards: Validators receive block rewards for proposing and validating blocks. These rewards are distributed from the network's inflationary issuance of AVAX tokens.

- Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This includes fees for simple transactions, smart contract interactions, and the creation of new assets on the network.

3. Penalties:

- Slashing: Unlike some other PoS systems, Avalanche does not employ slashing (i.e., the confiscation of staked tokens) as a penalty for misbehavior.Instead, the network relies on the financial disincentive of lost future rewards for validators who are not consistently online or act maliciously.

- Uptime Requirements: Validators must maintain a high level of uptime and correctly validate transactions to continue earning rewards. Poor performance or malicious actions result in missed rewards, providing a strong economic incentive to act honestly.

Fees on the Avalanche Blockchain

1. Transaction Fees:

- Dynamic Fees: Transaction fees on Avalanche are dynamic, varying based on network demand and the complexity of the transactions. This ensures that fees remain fair and proportional to the network's usage.

- Fee Burning: A portion of the transaction fees is burned, permanently removing them from circulation. This deflationary mechanism helps to balance the inflation from block rewards and incentivizes token holders by potentially increasing the value of AVAX over time.

2. Smart Contract Fees:

- Execution Costs: Fees for deploying and interacting with smart contracts are determined by the computational resources required. These fees ensure that the network remains efficient and that resources are used responsibly.

3. Asset Creation Fees:

- New Asset Creation: There are fees associated with creating new assets (tokens) on the Avalanche network. These fees help to prevent spam and ensure that only serious projects use the network's resources.

The following applies to Gnosis:

Validators on Gnosis earn GNO rewards for validating transactions and securing the network. Transaction fees are used to compensate for network resources and maintain stability.

The following applies to Near Protocol:

1. Validator incentives

- Validators must stake NEAR tokens in order to participate in block and chunk production.

- Validators receive epoch rewards every epoch (approximately 12 hours, or 43,200 blocks).

- The protocol targets an annual validator reward rate of approximately 2.5% to 4.5% of the total token supply, depending on how much NEAR is staked across the network.

- Rewards are socialized, meaning validators are paid based on their stake rather than the number of transactions or shards they directly process.

- Maximum annual protocol inflation is capped at 5%, of which 4.5% is used for validator rewards and 0.5% is allocated to the Protocol Treasury.

2. Transaction fees and fee burning

- Transaction fees on NEAR are paid in NEAR tokens.

- 100% of gas fees (after the developer rebate) are burned, permanently removing those tokens from circulation.

- 30% of the gas fees generated by a smart-contract call are automatically paid to the contract account as a developer rebate.

- Fee burning offsets inflation and may make the token supply deflationary during periods of high network usage.

3. Developer incentives

- Developers earn 30% of the gas fees generated when users interact with their smart contracts.

- These rewards are paid directly and automatically by the protocol, allowing developers to monetize applications without issuing their own tokens.

4. Storage staking incentives

- Users and developers must stake NEAR tokens to store data on-chain.

- The storage cost is approximately 1 NEAR per 100 kB of state.

- Tokens locked for storage cannot be used for validation staking, reducing the total circulating supply and indirectly increasing validator yields.

5. Slashing and economic penalties

- Validators risk losing their staked NEAR if they misbehave.

- Double signing results in progressive slashing, up to the full stake if a large portion of validators misbehave.

- Producing an invalid chunk results in 100% slashing of the validator’s stake.

- Validators that confirm erasure-coded land mines are immediately slashed.

- Validators that fail to meet production requirements can be removed from the active set through kickout thresholds.

6. Fishermen and protocol treasury

- Fishermen monitor the network and submit fraud proofs. They must post a 10 NEAR bond, which is lost if they submit false challenges.

- 10% of protocol inflation (approximately 0.5% of total supply per year) is allocated to a Protocol Treasury used to fund ecosystem development, infrastructure and education.

The following applies to Solana:

1. Validators:

Staking Rewards: Validators are chosen based on the number of SOL tokens they have staked. They earn rewards for producing and validating blocks, which are distributed in SOL. The more tokens staked, the higher the chances of being selected to validate transactions and produce new blocks.

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

2. Delegators:

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

3. Economic Security:

Slashing: Validators can be penalized for malicious behavior, such as producing invalid blocks or being frequently offline. This penalty, known as slashing, involves the loss of a portion of their staked tokens. Slashing is intended to deter dishonest actions and ensures that validators act in the best interest of the network.

Opportunity Cost: By staking SOL tokens, validators and delegators lock up their tokens, which could otherwise be used or sold. This opportunity cost is intended to incentivize participants to act honestly to earn rewards and avoid penalties.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana is designed to handle a high throughput of transactions, which is intended to keep the fees low and predictable.

Fee Structure: Fees are paid in SOL and are used to compensate validators for the resources they expend to process transactions. This includes computational power and network bandwidth.

2. Rent Fees:

State Storage: Solana charges so called ""rent fees"" for storing data on the blockchain. These fees are designed to discourage inefficient use of state storage and encourage developers to clean up unused state. Rent fees are intended to help maintain the efficiency and performance of the network.

3. Smart Contract Fees:

Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This is intended to ensure that users are charged proportionally for the resources they consume.

### H.6 Use of distributed ledger technology

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

### H.7 DLT functionality description

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

### H.8 Audit

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

### H.9 Audit outcome

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

## Part I – Information on risks

### I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service-provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

### I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

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

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

## I.4 Project implementation-related risks

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

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

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

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

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

## I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

### I.6 Mitigation measures

None.

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

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

### S.1 Name

Crypto Risk Metrics GmbH

### S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

### S.3 Name of the cryptoasset

Compound

### S.4 Consensus Mechanism

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

Core Components

1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an

entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security.

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

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

Consensus Process

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

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

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

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

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

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

The following applies to Avalanche C-Chain:

The Avalanche blockchain network employs a unique Proof-of-Stake consensus mechanism called Avalanche Consensus, which involves three interconnected protocols: Snowball, Snowflake, and Avalanche.

Avalanche Consensus Process:

1. Snowball Protocol:

- Random Sampling: Each validator randomly samples a small, constant-sized subset of other validators.

- Repeated Polling: Validators repeatedly poll the sampled validators to determine the preferred transaction.

- Confidence Counters: Validators maintain confidence counters for each transaction, incrementing them each time a sampled validator supports their preferred transaction.

- Decision Threshold: Once the confidence counter exceeds a pre-defined threshold, the transaction is considered accepted.

2. Snowflake Protocol:

- Binary Decision: Enhances the Snowball protocol by incorporating a binary decision process. Validators decide between two conflicting transactions.

- Binary Confidence: Confidence counters are used to track the preferred binary decision.

- Finality: When a binary decision reaches a certain confidence level, it becomes final.

3. Avalanche Protocol:

- DAG Structure: Uses a Directed Acyclic Graph (DAG) structure to organize transactions, allowing for parallel processing and higher throughput.

- Transaction Ordering: Transactions are added to the DAG based on their dependencies, ensuring a consistent order.

- Consensus on DAG: While most Proof-of-Stake Protocols use a Byzantine Fault Tolerant (BFT) consensus, Avalanche uses the Avalanche Consensus, Validators reach consensus on the structure and contents of the DAG through repeated Snowball and Snowflake.

The following applies to Gnosis:

Gnosis operates with a Proof-of-Stake (PoS) consensus mechanism, where validators secure the network by staking GNO tokens and participating in block production.

The following applies to Near Protocol:

1. Core consensus model

- NEAR does not use miners; instead, it relies on validators that stake NEAR tokens to participate in block and chunk production.

- Nightshade is a sharded consensus model in which all shards jointly produce a single logical block for each block height.

- Each shard produces a chunk containing transactions and state changes for that shard, and a designated block producer aggregates all chunks into one block.

2. Validator roles

- Block and Chunk Producers are responsible for creating blocks and producing shard chunks.

- Chunk Validators verify the correctness of chunks produced by other validators.

- Hidden Validators are randomly assigned to shards using a Verifiable Random Function (VRF) and verify chunk correctness without their assignment being known in advance.

- Fishermen are observing nodes that monitor the network and can submit fraud proofs if invalid behavior is detected.

3. Block production and finality

- Blocks and chunks are produced at an interval of approximately one second.

- Transactions become final once all related receipts (cross-shard execution messages) have been processed.

- Most transactions reach finality within 1 to 3 seconds, depending on cross-shard execution.

The following applies to Solana:

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

Core Concepts

1. Proof of History (PoH):

Time-Stamped Transactions: PoH is a cryptographic technique that timestamps transactions, intended to creating a historical record that proves that an event has occurred at a specific moment in time.

Verifiable Delay Function: PoH uses a Verifiable Delay Function (VDF) to generate a unique hash that includes the transaction and the time it was processed. This sequence of hashes provides a verifiable order of events, intended to enabling the network to efficiently agree on the sequence of transactions.

2. Proof of Stake (PoS):

Validator Selection: Validators are chosen to produce new blocks based on the number of SOL tokens they have staked. The more tokens staked, the higher the chance of being

selected to validate transactions and produce new blocks.

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

cryptographic clock for the network.

3. Block Production:

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

4. Consensus and Finalization:

Other validators verify the block produced by the leader validator. They check the correctness of the PoH sequence and validate the transactions within the block. Once the block is verified, it is added to the blockchain. Validators sign off on the block, and it is considered finalized.

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

Staking: Validators must stake SOL tokens to participate in the consensus process. This staking acts as collateral, incentivizing validators to act honestly. If a validator behaves maliciously or fails to perform, they risk losing their staked tokens.

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

3. Economic Penalties:

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

## S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is implemented on the Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana networks following the standards described below.

The following applies to Ethereum:

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

The following applies to Binance Smart Chain:

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

Incentive Mechanisms

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

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

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

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

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

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

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

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

The following applies to Avalanche C-Chain:

Avalanche uses a consensus mechanism known as Avalanche Consensus, which relies on a combination of validators, staking, and a novel approach to consensus to ensure the network's security and integrity.

1. Validators:

- Staking: Validators on the Avalanche network are required to stake AVAX tokens. The amount staked influences their probability of being selected to propose or validate new blocks.

- Rewards: Validators earn rewards for their participation in the consensus process. These rewards are proportional to the amount of AVAX staked and their uptime and performance in validating transactions.

- Delegation: Validators can also accept delegations from other token holders. Delegators share in the rewards based on the amount they delegate, which incentivizes smaller holders to participate indirectly in securing the network.

2. Economic Incentives:

- Block Rewards: Validators receive block rewards for proposing and validating blocks. These rewards are distributed from the network’s inflationary issuance of AVAX tokens.

- Transaction Fees: Validators also earn a portion of the transaction fees paid by users. This includes fees for simple transactions, smart contract interactions, and the creation of new assets on the network.

3. Penalties:

- Slashing: Unlike some other PoS systems, Avalanche does not employ slashing (i.e., the confiscation of staked tokens) as a penalty for misbehavior.Instead, the network relies on the financial disincentive of lost future rewards for validators who are not consistently online or act maliciously.

- Uptime Requirements: Validators must maintain a high level of uptime and correctly validate transactions to continue earning rewards. Poor performance or malicious actions result in missed rewards, providing a strong economic incentive to act honestly.

Fees on the Avalanche Blockchain

1. Transaction Fees:

- Dynamic Fees: Transaction fees on Avalanche are dynamic, varying based on network demand and the complexity of the transactions. This ensures that fees remain fair and proportional to the network's usage.

- Fee Burning: A portion of the transaction fees is burned, permanently removing them from circulation. This deflationary mechanism helps to balance the inflation from block rewards and incentivizes token holders by potentially increasing the value of AVAX over time.

2. Smart Contract Fees:

- Execution Costs: Fees for deploying and interacting with smart contracts are determined by the computational resources required. These fees ensure that the network remains efficient and that resources are used responsibly.

3. Asset Creation Fees:

- New Asset Creation: There are fees associated with creating new assets (tokens) on the Avalanche network. These fees help to prevent spam and ensure that only serious projects use the network's resources.

The following applies to Gnosis:

Validators on Gnosis earn GNO rewards for validating transactions and securing the network. Transaction fees are used to compensate for network resources and maintain stability.

The following applies to Near Protocol:

1. Validator incentives

- Validators must stake NEAR tokens in order to participate in block and chunk production.

- Validators receive epoch rewards every epoch (approximately 12 hours, or 43,200 blocks).

- The protocol targets an annual validator reward rate of approximately 2.5% to 4.5% of the total token supply, depending on how much NEAR is staked across the network.

- Rewards are socialized, meaning validators are paid based on their stake rather than the number of transactions or shards they directly process.

- Maximum annual protocol inflation is capped at 5%, of which 4.5% is used for validator rewards and 0.5% is allocated to the Protocol Treasury.

2. Transaction fees and fee burning

- Transaction fees on NEAR are paid in NEAR tokens.

- 100% of gas fees (after the developer rebate) are burned, permanently removing those tokens from circulation.

- 30% of the gas fees generated by a smart-contract call are automatically paid to the contract account as a developer rebate.

- Fee burning offsets inflation and may make the token supply deflationary during periods of high network usage.

3. Developer incentives

- Developers earn 30% of the gas fees generated when users interact with their smart contracts.

- These rewards are paid directly and automatically by the protocol, allowing developers to monetize applications without issuing their own tokens.

4. Storage staking incentives

- Users and developers must stake NEAR tokens to store data on-chain.

- The storage cost is approximately 1 NEAR per 100 kB of state.

- Tokens locked for storage cannot be used for validation staking, reducing the total circulating supply and indirectly increasing validator yields.

5. Slashing and economic penalties

- Validators risk losing their staked NEAR if they misbehave.

- Double signing results in progressive slashing, up to the full stake if a large portion of validators misbehave.

- Producing an invalid chunk results in 100% slashing of the validator’s stake.

- Validators that confirm erasure-coded land mines are immediately slashed.

- Validators that fail to meet production requirements can be removed from the active set through kickout thresholds.

6. Fishermen and protocol treasury

- Fishermen monitor the network and submit fraud proofs. They must post a 10 NEAR bond, which is lost if they submit false challenges.

- 10% of protocol inflation (approximately 0.5% of total supply per year) is allocated to a Protocol Treasury used to fund ecosystem development, infrastructure and education.

The following applies to Solana:

1. Validators:

Staking Rewards: Validators are chosen based on the number of SOL tokens they have staked. They earn rewards for producing and validating blocks, which are distributed in SOL. The more tokens staked, the higher the chances of being selected to validate transactions and produce new blocks.

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

2. Delegators:

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

3. Economic Security:

Slashing: Validators can be penalized for malicious behavior, such as producing invalid blocks or being frequently offline. This penalty, known as slashing, involves the loss of a portion of their staked tokens. Slashing is intended to deter dishonest actions and ensures that validators act in the best interest of the network.

Opportunity Cost: By staking SOL tokens, validators and delegators lock up their tokens, which could otherwise be used or sold. This opportunity cost is intended to incentivize participants to act honestly to earn rewards and avoid penalties.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana is designed to handle a high throughput of transactions, which is intended to keep the fees low and predictable.

Fee Structure: Fees are paid in SOL and are used to compensate validators for the resources they expend to process transactions. This includes computational power and network bandwidth.

2. Rent Fees:

State Storage: Solana charges so called ""rent fees"" for storing data on the blockchain. These fees are designed to discourage inefficient use of state storage and encourage developers to clean up unused state. Rent fees are intended to help maintain the efficiency and performance of the network.

3. Smart Contract Fees:

Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This is intended to ensure that users are charged proportionally for the resources they consume.

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

2025-01-22

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

2026-01-22

### S.8 Energy consumption

449.32617 kWh/a

### S.9 Energy consumption sources and methodologies

The energy consumption associated with this crypto-asset is aggregated of multiple contributing components, primarily the underlying blockchain network and the execution of token-specific operations. To determine the energy consumption of a token, the energy consumption of the underlying blockchain networks Ethereum, Binance Smart Chain, Avalanche C-Chain, Gnosis Chain, Near Protocol and Solana is calculated first. A proportionate share of that energy use is then attributed to the token based on its activity level within the network (e.g. transaction volume, contract execution).

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

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

### S.10 Renewable energy consumption

34.5110684726 %

### S.11 Energy intensity

0.00002 kWh

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

0.00000 tCO2e/a

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

0.14954 tCO2e/a

### S.14 GHG intensity

0.00000 kgCO2e

### S.15 Key energy sources and methodologies

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

### S.16 Key GHG sources and methodologies

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.