

**White paper drafted under the  
European Markets in Crypto-  
Assets Regulation (EU)  
2023/1114 for FFG 75D0KJ7WN**

## Preamble

### 00. Table of Contents

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

|                                                                                                                                                                                                                                                                              |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Part B – Information about the issuer, if different from the offeror or person seeking admission to trading                                                                                                                                                                  | 12 |
| B.1 Issuer different from offeror or person seeking admission to trading                                                                                                                                                                                                     | 12 |
| B.2 Name                                                                                                                                                                                                                                                                     | 12 |
| B.3 Legal form                                                                                                                                                                                                                                                               | 12 |
| B.4 Registered address                                                                                                                                                                                                                                                       | 12 |
| B.5 Head office                                                                                                                                                                                                                                                              | 13 |
| B.6 Registration date                                                                                                                                                                                                                                                        | 13 |
| B.7 Legal entity identifier                                                                                                                                                                                                                                                  | 13 |
| B.8 Another identifier required pursuant to applicable national law                                                                                                                                                                                                          | 13 |
| B.9 Parent company                                                                                                                                                                                                                                                           | 13 |
| B.10 Members of the management body                                                                                                                                                                                                                                          | 13 |
| B.11 Business activity                                                                                                                                                                                                                                                       | 13 |
| B.12 Parent company business activity                                                                                                                                                                                                                                        | 13 |
| Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 | 13 |
| C.1 Name                                                                                                                                                                                                                                                                     | 13 |
| C.2 Legal form                                                                                                                                                                                                                                                               | 13 |
| C.3 Registered address                                                                                                                                                                                                                                                       | 14 |
| C.4 Head office                                                                                                                                                                                                                                                              | 14 |
| C.5 Registration date                                                                                                                                                                                                                                                        | 14 |
| C.6 Legal entity identifier                                                                                                                                                                                                                                                  | 14 |
| C.7 Another identifier required pursuant to applicable national law                                                                                                                                                                                                          | 14 |
| C.8 Parent company                                                                                                                                                                                                                                                           | 14 |
| C.9 Reason for crypto-asset white paper preparation                                                                                                                                                                                                                          | 14 |
| C.10 Members of the management body                                                                                                                                                                                                                                          | 14 |
| C.11 Operator business activity                                                                                                                                                                                                                                              | 14 |
| C.12 Parent company business activity                                                                                                                                                                                                                                        | 14 |
| C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114                                                                                                                                      | 14 |
| C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114                                                                                                                                            | 14 |
| Part D – Information about the crypto-asset project                                                                                                                                                                                                                          | 14 |
| D.1 Crypto-asset project name                                                                                                                                                                                                                                                | 14 |
| D.2 Crypto-assets name                                                                                                                                                                                                                                                       | 15 |
| D.3 Abbreviation                                                                                                                                                                                                                                                             | 15 |

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| D.4 Crypto-asset project description                                                                   | 15 |
| D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project | 15 |
| D.6 Utility Token Classification                                                                       | 15 |
| D.7 Key Features of Goods/Services for Utility Token Projects                                          | 16 |
| D.8 Plans for the token                                                                                | 16 |
| D.9 Resource allocation                                                                                | 16 |
| D.10 Planned use of collected funds or crypto-assets                                                   | 17 |
| Part E – Information about the offer to the public of crypto-assets or their admission to trading      | 17 |
| E.1 Public offering or admission to trading                                                            | 17 |
| E.2 Reasons for public offer or admission to trading                                                   | 17 |
| E.3 Fundraising target                                                                                 | 17 |
| E.4 Minimum subscription goals                                                                         | 17 |
| E.5 Maximum subscription goals                                                                         | 17 |
| E.6 Oversubscription acceptance                                                                        | 17 |
| E.7 Oversubscription allocation                                                                        | 17 |
| E.8 Issue price                                                                                        | 17 |
| E.9 Official currency or any other crypto-assets determining the issue price                           | 18 |
| E.10 Subscription fee                                                                                  | 18 |
| E.11 Offer price determination method                                                                  | 18 |
| E.12 Total number of offered/traded crypto-assets                                                      | 18 |
| E.13 Targeted holders                                                                                  | 18 |
| E.14 Holder restrictions                                                                               | 18 |
| E.15 Reimbursement notice                                                                              | 18 |
| E.16 Refund mechanism                                                                                  | 18 |
| E.17 Refund timeline                                                                                   | 18 |
| E.18 Offer phases                                                                                      | 18 |
| E.19 Early purchase discount                                                                           | 19 |
| E.20 Time-limited offer                                                                                | 19 |
| E.21 Subscription period beginning                                                                     | 19 |
| E.22 Subscription period end                                                                           | 19 |
| E.23 Safeguarding arrangements for offered funds/crypto-assets                                         | 19 |
| E.24 Payment methods for crypto-asset purchase                                                         | 19 |
| E.25 Value transfer methods for reimbursement                                                          | 19 |
| E.26 Right of withdrawal                                                                               | 19 |
| E.27 Transfer of purchased crypto-assets                                                               | 19 |

|                                                                                                                                                                                                                                                                                |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| E.28 Transfer time schedule                                                                                                                                                                                                                                                    | 19 |
| E.29 Purchaser's technical requirements                                                                                                                                                                                                                                        | 19 |
| E.30 Crypto-asset service provider (CASP) name                                                                                                                                                                                                                                 | 20 |
| E.31 CASP identifier                                                                                                                                                                                                                                                           | 20 |
| E.32 Placement form                                                                                                                                                                                                                                                            | 20 |
| E.33 Trading platforms name                                                                                                                                                                                                                                                    | 20 |
| E.34 Trading platforms Market identifier code (MIC)                                                                                                                                                                                                                            | 20 |
| E.35 Trading platforms access                                                                                                                                                                                                                                                  | 20 |
| E.36 Involved costs                                                                                                                                                                                                                                                            | 20 |
| E.37 Offer expenses                                                                                                                                                                                                                                                            | 20 |
| E.38 Conflicts of interest                                                                                                                                                                                                                                                     | 20 |
| E.39 Applicable law                                                                                                                                                                                                                                                            | 21 |
| E.40 Competent court                                                                                                                                                                                                                                                           | 21 |
| Part F – Information about the crypto-assets                                                                                                                                                                                                                                   | 21 |
| F.1 Crypto-asset type                                                                                                                                                                                                                                                          | 21 |
| F.2 Crypto-asset functionality                                                                                                                                                                                                                                                 | 21 |
| F.3 Planned application of functionalities                                                                                                                                                                                                                                     | 21 |
| 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 | 22 |
| F.4 Type of crypto-asset white paper                                                                                                                                                                                                                                           | 22 |
| F.5 The type of submission                                                                                                                                                                                                                                                     | 22 |
| F.6 Crypto-asset characteristics                                                                                                                                                                                                                                               | 22 |
| F.7 Commercial name or trading name                                                                                                                                                                                                                                            | 22 |
| F.8 Website of the issuer                                                                                                                                                                                                                                                      | 22 |
| F.9 Starting date of offer to the public or admission to trading                                                                                                                                                                                                               | 22 |
| F.10 Publication date                                                                                                                                                                                                                                                          | 22 |
| F.11 Any other services provided by the issuer                                                                                                                                                                                                                                 | 22 |
| F.12 Language or languages of the crypto-asset white paper                                                                                                                                                                                                                     | 23 |
| 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                                                                                                                            | 23 |
| F.14 Functionally fungible group digital token identifier                                                                                                                                                                                                                      | 23 |
| F.15 Voluntary data flag                                                                                                                                                                                                                                                       | 23 |
| F.16 Personal data flag                                                                                                                                                                                                                                                        | 23 |
| F.17 LEI eligibility                                                                                                                                                                                                                                                           | 23 |
| F.18 Home Member State                                                                                                                                                                                                                                                         | 23 |
| F.19 Host Member States                                                                                                                                                                                                                                                        | 23 |

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Part G – Information on the rights and obligations attached to the crypto-assets | 23 |
| G.1 Purchaser rights and obligations                                             | 23 |
| G.2 Exercise of rights and obligations                                           | 24 |
| G.3 Conditions for modifications of rights and obligations                       | 24 |
| G.4 Future public offers                                                         | 24 |
| G.5 Issuer retained crypto-assets                                                | 24 |
| G.6 Utility token classification                                                 | 25 |
| G.7 Key features of goods/services of utility tokens                             | 25 |
| G.8 Utility tokens redemption                                                    | 25 |
| G.9 Non-trading request                                                          | 25 |
| G.10 Crypto-assets purchase or sale modalities                                   | 25 |
| G.11 Crypto-assets transfer restrictions                                         | 25 |
| G.12 Supply adjustment protocols                                                 | 25 |
| G.13 Supply adjustment mechanisms                                                | 25 |
| G.14 Token value protection schemes                                              | 25 |
| G.15 Token value protection schemes description                                  | 26 |
| G.16 Compensation schemes                                                        | 26 |
| G.17 Compensation schemes description                                            | 26 |
| G.18 Applicable law                                                              | 26 |
| G.19 Competent court                                                             | 26 |
| Part H – information on the underlying technology                                | 26 |
| H.1 Distributed ledger technology (DLT)                                          | 26 |
| H.2 Protocols and technical standards                                            | 26 |
| H.3 Technology used                                                              | 29 |
| H.4 Consensus mechanism                                                          | 29 |
| H.5 Incentive mechanisms and applicable fees                                     | 31 |
| H.6 Use of distributed ledger technology                                         | 32 |
| H.7 DLT functionality description                                                | 32 |
| H.8 Audit                                                                        | 33 |
| H.9 Audit outcome                                                                | 33 |
| Part I – Information on risks                                                    | 33 |
| I.1 Offer-related risks                                                          | 33 |
| I.2 Issuer-related risks                                                         | 35 |
| I.3 Crypto-assets-related risks                                                  | 36 |
| I.4 Project implementation-related risks                                         | 39 |
| I.5 Technology-related risks                                                     | 39 |

|                                                                                                                                                  |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----|
| I.6 Mitigation measures                                                                                                                          | 42 |
| Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts | 42 |
| J.1 Adverse impacts on climate and other environment-related adverse impacts                                                                     | 42 |
| S.1 Name                                                                                                                                         | 42 |
| S.2 Relevant legal entity identifier                                                                                                             | 42 |
| S.3 Name of the crypto-asset                                                                                                                     | 42 |
| S.4 Consensus Mechanism                                                                                                                          | 42 |
| S.5 Incentive Mechanisms and Applicable Fees                                                                                                     | 44 |
| S.6 Beginning of the period to which the disclosure relates                                                                                      | 45 |
| S.7 End of the period to which the disclosure relates                                                                                            | 45 |
| S.8 Energy consumption                                                                                                                           | 45 |
| S.9 Energy consumption sources and methodologies                                                                                                 | 45 |
| S.10 Renewable energy consumption                                                                                                                | 46 |
| S.11 Energy intensity                                                                                                                            | 46 |
| S.12 Scope 1 DLT GHG emissions – Controlled                                                                                                      | 46 |
| S.13 Scope 2 DLT GHG emissions – Purchased                                                                                                       | 46 |
| S.14 GHG intensity                                                                                                                               | 46 |
| S.15 Key energy sources and methodologies                                                                                                        | 46 |
| S.16 Key GHG sources and methodologies                                                                                                           | 46 |

## **01. Date of notification**

This white paper was notified on 2026-08-18.

## **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 Peanut the Squirrel (PNUT) referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed on the Solana network according to the DTI FFG shown in section F.14, as of 2026-08-13. The maximum supply of the crypto-asset is 1,000,000,000 tokens. The first activity on Solana can be viewed on 2024-10-31 (transaction hash: 2Av1bHTDCSc9hU5nNHfFmn2xUujftEV4HcwSszU6v5Axrf46vaGWbLjmTYysHkcv9ajsUpzWjF61VZaQE1EUWWme, source: <https://solscan.io/tx/2Av1bHTDCSc9hU5nNHfFmn2xUujftEV4HcwSszU6v5Axrf46vaGWbLjmTYysHkcv9ajsUpzWjF61VZaQE1EUWWme>, accessed 2026-08-13).

The project is associated with the PNUT crypto-asset and with internet meme culture linked to the rescued animal known as Peanut the Squirrel. The crypto-asset may be used for peer-to-peer transfers on the Solana network and may be held in compatible Solana wallets. Based on the information provided, PNUT does not have a specific blockchain-based protocol function beyond its existence as an SPL token associated with its branding and cultural references. It is not described as being required for network fees, staking, protocol security or governance of an underlying PNUT-specific blockchain or protocol.

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

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

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

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

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

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

### **A.1 Name**

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

## **A.2 Legal form**

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

## **A.3 Registered address**

The registered address of Crypto Risk Metrics GmbH is Lange Reihe 73, 20099 Hamburg, Germany,  
federal state of Hamburg.

## **A.4 Head office**

The head office is identical to the registered address.

## **A.5 Registration date**

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

## **A.6 Legal entity identifier**

The Legal Entity Identifier (LEI) of Crypto Risk Metrics GmbH is 39120077M9TG001FE242.

## **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 Zölit | Chairman | Lange Reihe 73, 20099 Hamburg, Germany |

## **A.13 Business activity**

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

1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, Crypto Risk Metrics GmbH aims to provide central services for crypto-asset white papers.

#### **A.14 Parent company business activity**

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

#### **A.15 Newly established**

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

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

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

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

#### **A.17 Financial condition since registration**

Not applicable

### **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**

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. No registered legal-entity issuer has been identified. This does not prevent the issuer from being sufficiently identifiable in the future. In certain cases, legal entities, organised development teams, or natural persons may take central positions around a crypto-asset project and may therefore be considered relevant for the assessment of the issuer or issuer-like functions. In the present case, the account HrHJputHcA8mkwrcQB3GkrJ2u1f7Fm4LzAZptSYSsUcf created the crypto-asset on the Solana blockchain on 31 October 2024, acquired 63,909,090 units, being 6.39 per cent of the total supply, in the same transaction, and disposed of that entire holding approximately two minutes later. The account has not been publicly attributed to any identified natural or legal person, and no continuing holding, control or governance function connected to it has been identified. Such persons or structures may therefore be relevant for the assessment of issuer-like functions in relation to the crypto-asset.

#### **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**

Not applicable, as no registered legal-entity issuer has been identified.

### **B.7 Legal entity identifier**

Not applicable, as no registered legal-entity issuer has been identified.

### **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**

| <b>Identity</b> | <b>Function</b> | <b>Business Address</b> |
|-----------------|-----------------|-------------------------|
| 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: "Peanut the Squirrel", Short Name: "PNUT" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2026-08-13).

## D.2 Crypto-assets name

Long Name: "Peanut the Squirrel" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2026-08-13).

## D.3 Abbreviation

Short Name: "PNUT" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2026-08-13).

## D.4 Crypto-asset project description

PNUT is a meme-based crypto-asset created through Pump.fun on the Solana blockchain on 31 October 2024. Its name and theme refer to Peanut the Squirrel, a rescued animal whose seizure and euthanasia by New York State authorities attracted widespread public attention and online discussion.

The project uses this story as its principal cultural theme. PNUT may be held and transferred as a fungible crypto-asset, but it does not provide access to goods or services and has no stated functionality beyond holding and transfer.

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure, and publicly available information does not identify a formal project company, foundation or management body. Natural persons, legal persons, undertakings, organised development teams, governance arrangements, or other project-related structures connected to the crypto-asset project may nonetheless be relevant for the assessment of issuer-like functions, to the extent such persons or structures can be identified from available information. The available project materials do not describe an on-chain governance system or a token-holder voting mechanism.

The long-term evolution of the project depends on technical, economic and regulatory considerations, and all future developments remain subject to change.

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

| Name of person                                                                                                 | Type of person                          | Business address of person | Domicile of company |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------|----------------------------|---------------------|
| Person controlling Solana account HrHJputHcA8mkwrcQB3GkrJ2u1f7Fm4LzAZptSYSsUcf, which created the crypto-asset | Other person involved in implementation | Cannot be found            | Cannot be found     |

## D.6 Utility Token Classification

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

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

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

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

## **D.8 Plans for the token**

The crypto-asset was created as a meme token and no roadmap, development plan or other plans for the crypto-asset have been published. The publicly available project materials are limited to information about the origin of the crypto-asset and instructions for acquiring it, and do not set out any planned development.

The project has not published a formal roadmap and has not communicated any concrete technical, functional or utility development plans for the PNUT token.

## **D.9 Resource allocation**

The crypto-asset was created as a meme token and its development has not been funded through any fundraising process. The entire supply of 1,000,000,000 units was generated at the mint on 31 October 2024 through a permissionless token launch platform on the Solana blockchain. No initial coin offering, no public or private token sale and no seed, venture or other equity funding round has been identified. No development budget, treasury, grant programme or allocation schedule has been published, and no resources are held for allocation to the crypto-asset project.

The initial distribution occurred through the launch platform's bonding curve mechanism. The account that created the crypto-asset acquired 63,909,090 units, being 6.39 per cent of the total supply, in the same transaction as the mint, and disposed of that entire holding approximately two minutes later for 3.516319267 SOL, equivalent to approximately USD 620 at the SOL exchange rate prevailing on 31 October 2024. As at 13 August 2026, that account held 83 units of the crypto-asset, being less than 0.00001 per cent of the total supply.

The token distribution can be traced on-chain on Solana: <https://solscan.io/token/2qEHjDLDLbuBgRYvsxhc5D6uDWAivNFZGan56P1tpump#holders>. The investor must be aware that a public address cannot necessarily be assigned to a single person or entity, which limits the ability to determine exact economic influence or future actions.

The natural persons, legal persons, undertakings, organised development teams, governance arrangements or other structures connected to the PNUT crypto-asset project have not independently confirmed the occurrence, precise amounts or current status of these reported allocations and fundraising figures. As a result, the referenced allocation figures cannot be



independently verified and should be considered indicative only. Token distribution changes can negatively impact the investor.

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

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

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

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

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

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

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

## **E.3 Fundraising target**

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

## **E.4 Minimum subscription goals**

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

## **E.5 Maximum subscription goals**

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

## **E.6 Oversubscription acceptance**

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

## **E.7 Oversubscription allocation**

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

## **E.8 Issue price**

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

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

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

## **E.10 Subscription fee**

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

## **E.11 Offer price determination method**

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

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

A total of 1,000,000,000 units were minted on 31 October 2024, as recorded in the mint transaction on the Solana blockchain (<https://solscan.io/tx/2Av1bHTDCSc9hU5nNHfFmn2xUujftEV4HcwSszU6v5Axrf46vaGWbLjmTYysHkcv9ajsUpzWjF61VZaQE1EUWWme>, accessed 2026-08-13).

Investors should be aware that changes in the effective supply, whether through increases in the circulating units or reductions through burning, may affect the price and liquidity of the crypto-asset.

## **E.13 Targeted holders**

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

## **E.14 Holder restrictions**

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

## **E.15 Reimbursement notice**

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

## **E.16 Refund mechanism**

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

## **E.17 Refund timeline**

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

## **E.18 Offer phases**

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

### **E.19 Early purchase discount**

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

### **E.20 Time-limited offer**

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

### **E.21 Subscription period beginning**

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

### **E.22 Subscription period end**

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

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

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

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

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

### **E.25 Value transfer methods for reimbursement**

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

### **E.26 Right of withdrawal**

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

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

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

### **E.28 Transfer time schedule**

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

### **E.29 Purchaser's technical requirements**

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

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

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

### **E.31 CASP identifier**

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

### **E.32 Placement form**

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

### **E.33 Trading platforms name**

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

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

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

### **E.35 Trading platforms access**

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

### **E.36 Involved costs**

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

### **E.37 Offer expenses**

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

### **E.38 Conflicts of interest**

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

Crypto Risk Metrics GmbH has established, implemented, and documented comprehensive internal policies and procedures for the identification, prevention, management, and documentation of conflicts of interest in accordance with applicable regulatory requirements. These internal measures

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

### **E.39 Applicable law**

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

### **E.40 Competent court**

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

## **Part F – Information about the crypto-assets**

### **F.1 Crypto-asset type**

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

### **F.2 Crypto-asset functionality**

PNUT is a fungible token created through Pump.fun using the Solana Token Program and is commonly referred to as an SPL token. Its functionality is limited to being held in compatible Solana wallets and transferred between token accounts on the Solana network. PNUT does not provide access to any goods or services and has no separate application or technical functionality beyond these standard token operations.

PNUT does not confer ownership, profit participation, redemption rights, governance rights over any issuer or related entity in a corporate-law sense, or any other legally enforceable economic entitlement. Its usability depends on the operation, availability and technical conditions of the Solana network and compatible wallet infrastructure, which are outside the control of token holders.

### **F.3 Planned application of functionalities**

The project has not published a formal roadmap and has not communicated any concrete technical, functional or utility development plans for the PNUT token.

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

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

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

**F.5 The type of submission**

The type of submission is MODI (Modified white paper).

**F.6 Crypto-asset characteristics**

PNUT is a crypto-asset other than an e-money token (EMT) or an asset-referenced token (ART) and is issued on the Solana blockchain. It is fungible and divisible to six decimal places. The initial mint created 1,000,000,000 PNUT. PNUT constitutes a digital representation of value recorded using distributed ledger technology. It does not confer ownership, profit participation, governance or other legally enforceable rights. Its functionality is limited to standard holding and transfer operations on the Solana network. These technical operations do not constitute contractual entitlements and depend on the operation and availability of the Solana network. PNUT is not backed by assets or a mechanism designed to protect its value. Its market value is determined by market factors, including supply, demand, liquidity and market sentiment.

**F.7 Commercial name or trading name**

Long Name: "Peanut the Squirrel" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2026-08-13).

**F.8 Website of the issuer**

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, no website of a registered legal-entity issuer has been identified.

General information about the underlying project is made publicly available at: <https://pnutsol.com/>. This website should not be understood as the website of a registered legal-entity issuer within the meaning of Regulation (EU) 2023/1114 (MiCA).

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

2025-06-30

**F.10 Publication date**

2025-06-30

**F.11 Any other services provided by the issuer**

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Therefore, no other services provided by a registered legal-entity issuer have been identified.

It cannot be excluded that natural persons, organised development teams, or other structures connected to the crypto-asset project provide or may provide additional services 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**

7FJ0P4TBH

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

75D0KJ7WN

## **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 (the GDPR).

## **F.17 LEI eligibility**

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, no registered legal-entity issuer has been identified for which LEI eligibility could be assessed.

## **F.18 Home Member State**

Germany

## **F.19 Host Member States**

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

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

## **G.1 Purchaser rights and obligations**

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

Accordingly, holders do not acquire any legally enforceable claim against the issuer of the crypto-asset or any third party.

## **G.2 Exercise of rights and obligations**

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

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

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

## **G.4 Future public offers**

Information on future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-08-13).

## **G.5 Issuer retained crypto-assets**

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, no retained holding attributable to a registered legal-entity issuer has been identified, and no publicly disclosed vesting schedule or lock-up arrangement has been identified.

The account HrHJputHcA8mkwrcQB3GkrJ2u1f7Fm4LzAZptSYsUcf created the crypto-asset on the Solana blockchain on 31 October 2024 and is the only account that has been identified as connected to issuer-like functions in relation to the crypto-asset. That account acquired 63,909,090 units, being 6.39 per cent of the total supply, in the same transaction as the mint, and disposed of that entire holding approximately two minutes later. As at 13 August 2026, that account held 83 units of the crypto-asset, being less than 0.00001 per cent of the total supply.

The token distribution can be traced on-chain on Solana: <https://solscan.io/token/2qEHjDLDLbuBgRYvsxhc5D6uDWAivNFZGan56P1tpump#holders>. The investor must be aware that a public address cannot necessarily be assigned to a single person or entity, which limits the ability to determine exact economic influence or future actions.

For the same reason, it cannot be excluded that natural persons, legal persons, undertakings, organised development teams, governance arrangements, or other project-related structures connected to the crypto-asset control further addresses through which units of the crypto-asset have been acquired, held or disposed of. Any such addresses have not been identified and the holdings associated with them cannot be quantified.



The information presented in this section is based on publicly available information, should be considered indicative only, and changes in the holdings of project-related persons or structures can negatively impact the investor.

## **G.6 Utility token classification**

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

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

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

## **G.8 Utility tokens redemption**

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

## **G.9 Non-trading request**

The admission to trading is sought.

## **G.10 Crypto-assets purchase or sale modalities**

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

## **G.11 Crypto-assets transfer restrictions**

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

## **G.12 Supply adjustment protocols**

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-08-13.

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

## **G.13 Supply adjustment mechanisms**

Not applicable.

## **G.14 Token value protection schemes**

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

### **G.15 Token value protection schemes description**

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

### **G.16 Compensation schemes**

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

### **G.17 Compensation schemes description**

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

### **G.18 Applicable law**

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

### **G.19 Competent court**

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

## **Part H – information on the underlying technology**

### **H.1 Distributed ledger technology (DLT)**

The crypto-asset in scope is implemented on the Solana network following the standards described below.

### **H.2 Protocols and technical standards**

The crypto-asset that is the subject of this white paper is available on the Solana network.

The following applies to Solana:

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

#### **1. Network Architecture and Core Protocols**

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

- Solana uses Proof-of-History (PoH) as a cryptographic timing and ordering mechanism, while validator participation and voting are stake-weighted under its Proof-of-Stake model and Tower BFT consensus process.
- Tower BFT: A Byzantine fault tolerant consensus mechanism, derived from PBFT, that governs validator voting and block confirmation.
- Turbine: A block propagation protocol that distributes blocks across the validator network by splitting them into smaller data fragments ("shreds") and transmitting them through a layered tree-based structure.
- Gulf Stream: A transaction forwarding mechanism that routes transactions directly to upcoming block producers and thereby limits the need for a global transaction mempool.
- Sealevel: A parallel transaction execution engine that enables non-conflicting transactions and programs to execute simultaneously across multiple processing threads.

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

## 2. Address and Cryptographic Standards

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

- Account Addresses: Accounts are identified by 32-byte addresses. Externally controlled accounts typically use Ed25519 key pairs, while program-derived addresses (PDAs) are deterministically derived off-curve addresses that do not correspond to a private key.
- Transaction Signatures: Transactions are authorised through Ed25519 signatures associated with the account owner's keypair.
- Hashing: Sequential SHA-256 hashing is used within the Proof-of-History mechanism to generate a verifiable ordering of events.
- Program Derived Addresses (PDAs): Deterministically generated addresses derived through hashing procedures that ensure the resulting address does not correspond to a private key, thereby enabling secure program-controlled accounts.

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

## 3. Networking and Data Transmission Standards

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

- QUIC is used for transaction ingress and TPU-related forwarding paths on Solana validators, alongside other networking channels used across the cluster.
- UDP-based propagation: Utilised for distributing block fragments ("shreds") across the network through the Turbine protocol.
- Transaction size limits: The maximum transaction size of approximately 1,232 bytes is aligned with the IPv6 minimum transmission unit (MTU) after accounting for network headers, and is intended to enable atomic transmission without fragmentation.
- JSON-RPC interfaces: Standardised APIs used by wallets, applications, and infrastructure providers to submit transactions and query blockchain state.

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

#### 4. Token and Program Standards (Solana Program Library)

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

Within this framework:

- A token type is represented by a mint account, which defines parameters such as total supply and mint authority.
- Individual token balances are stored in token accounts, which hold balances associated with a specific mint and owner address.
- Interactions with tokens occur through instructions executed by the relevant token program rather than through separate token-specific smart contracts.

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

#### 5. Protocol Development and Improvement Standards

Technical changes to the Solana protocol may be proposed and discussed through Solana Improvement Documents (SIMDs). These proposals document suggested modifications to protocol

behaviour, economic parameters, or technical limits. Accepted changes may be implemented through updates to validator software and related developer tooling used by network participants.

### **H.3 Technology used**

The crypto-asset that is the subject of this white paper is available on the Solana network.

The following applies to Solana:

1. Solana-Compatible Wallets: The tokens are generally supported by wallets compatible with Solana's token programs.
2. Decentralised Ledger: The Solana blockchain acts as a decentralised ledger for all token transactions, with the intention of preserving a tamper-resistant record of token transfers and ownership in order to ensure both transparency and security.
3. SPL Token Program: Tokens on Solana are commonly implemented using either the original Token Program or the Token Extension Program (Token-2022), which provide standardised on-chain logic for token creation, issuance, transfer, and account management. Unlike the ERC-20 model on Ethereum, where a project typically deploys its own token contract, Solana tokens generally rely on shared token-program infrastructure, which promotes a high degree of standardisation across the ecosystem.
4. Blockchain Scalability: Solana is designed to support high transaction throughput and comparatively low transaction fees, with the intention of enabling efficient token transfers and related on-chain operations.

Security Protocols for Asset Custody and Transactions:

1. Private Key Management: To safeguard their token holdings, users must securely store their wallet's private keys and recovery phrases.
2. Cryptographic Integrity: Solana uses Ed25519 digital signatures to authenticate transactions submitted by authorised signers, thereby supporting the integrity and verifiability of token transfers.

### **H.4 Consensus mechanism**

The crypto-asset that is the subject of this white paper is available on the Solana network.

The following applies to Solana:

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

Core Concepts

## 1. Proof-of-History (PoH):

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

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

## 2. Proof-of-Stake (PoS):

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

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

## Consensus Process

### 1. Transaction Validation:

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

### 2. PoH Sequence Generation:

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

### 3. Block Production:

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

### 4. Consensus and Finalisation:

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

## Security and Economic Incentives

### 1. Incentives for Validators:

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

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

### 2. Security:

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

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

### 3. Economic Penalties:

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

## **H.5 Incentive mechanisms and applicable fees**

The crypto-asset that is the subject of this white paper is available on the Solana network.

The following applies to Solana:

### 1. Validators:

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

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

## 2. Delegators:

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

## 3. Economic Security:

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

## Fees Applicable on the Solana Blockchain

### 1. Transaction Fees:

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

### 2. Rent Fees:

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

### 3. Program Execution Costs:

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

## **H.6 Use of distributed ledger technology**

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

## **H.7 DLT functionality description**

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



## H.8 Audit

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

## H.9 Audit outcome

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

# Part I – Information on risks

## I.1 Offer-related risks

### 1. Regulatory and Compliance

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

### 2. Trading venue and connection risk

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

### 3. Market formation and liquidity conditions

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

**Volatility:** The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or

DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the crypto-asset at or close to a previously observed price, even where no negative project-specific event has occurred.

#### 4. Counterparty and service provider dependence

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

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

**Delisting and service suspension:** The crypto-asset's availability may depend on the internal listing decisions of these counterparties. Such decisions may be influenced by factors unconnected with the technical operation of the crypto-asset, including pending legal proceedings concerning the crypto-asset subject of this white paper or the platform through which it was created, claims asserted by third parties in respect of the name, ticker symbol or imagery associated with it, or supervisory warnings addressed to parties connected with it. A delisting or suspension on a key connected venue can materially reduce liquidity or make trading temporarily impossible on the admitting service provider, even if the underlying crypto-asset continues to function.

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

#### 5. Operational and information risks

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

#### 6. Market access and liquidity concentration risk

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

## **I.2 Issuer-related risks**

Interpretative note for this section: The risk factors set out in this Part I.2 follow the structure of the applicable MiCA white paper template for crypto-assets other than asset-referenced tokens or e-money tokens under Title II of MiCA, including references to issuer-related risks. For the purposes of this Part I.2, references to an “issuer”, “issuer-related risks” or similar terms should be read in line with the definition of “issuer” under MiCA, including any natural or legal person, or other undertaking, that issues crypto-assets.

Based on the available information, the crypto-asset does not appear to be issued through a traditional corporate, foundation, or comparable legal entity structure. Accordingly, the risk descriptions in this Part I.2 should be understood as referring, as applicable, to any natural persons, legal persons, undertakings, organised development teams, governance arrangements, or other project-related structures that may materially influence the crypto-asset or the related project, to the extent such persons or structures can be identified from available information.

### **1. Absence or insolvency of an identifiable issuer**

Where an identifiable issuer exists, that issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, legal or regulatory developments, or external shocks, including pandemics or armed conflicts. In such a case, ongoing development, support, communication, or governance of the crypto-asset project may be reduced, suspended, or discontinued, potentially affecting the viability, availability, market acceptance, or 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 subject of this white paper provides no access to any good or service and has no functionality beyond being held and transferred. It confers no entitlement to revenue, fees or distributions of any kind, and no proceeds of trading in it accrue to holders by virtue of holding. Its market value is therefore driven solely by supply and demand, which in turn depend on continuing public attention to the cultural theme with which it is associated, and may fluctuate significantly.

#### 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. Crypto-assets of this type have historically exhibited pronounced price movements over very short periods, including rapid appreciation during an initial period of elevated public attention followed by substantial and sustained decline. Holders should not assume that previously observed price levels are indicative of future levels.

#### 3. Liquidity and price-determination risk

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

#### 4. Crypto-asset security risk

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

#### 5. Fraud and scam risk

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

#### 6. Legal and regulatory reclassification risk

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

In January 2025, civil class action proceedings were commenced before the United States District Court for the Southern District of New York on behalf of all purchasers of the crypto-asset subject of this white paper. The claimants allege that it is a security within the meaning of the United States Securities Act of 1933, that no registration statement was filed in respect of it, and that the operator of the platform through which it was first sold and individuals alleged to control that operator are liable for selling and soliciting the sale of unregistered securities. Those proceedings were consolidated with related proceedings in June 2025 and the operative complaint in the consolidated proceedings was filed in January 2026. The claimants seek damages and other relief on behalf of purchasers.

The allegations are contested, no court has determined that the crypto-asset is a security, and nothing in these proceedings constitutes a finding of liability. The outcome cannot be predicted. An adverse determination, or a settlement or other measure adopted in response to the proceedings, could restrict the offering, trading or custody of the crypto-asset in the United States, could influence how other authorities and trading venues treat it, and could adversely affect confidence in or demand for it.

#### 7. Absence of investor protection

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

#### 8. Counterparty risk

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

## 9. Reputational risk

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

## 10. Community and sentiment risk

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

## 11. Macroeconomic and interest-rate risk

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

## 12. Taxation risk

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

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

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

## 14. Market-abuse risk

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

## 15. Legal ownership and jurisdictional risk

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

## 16. Concentration risk

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

#### 17. Intellectual property risk

Rights in the name, ticker symbol and imagery associated with the crypto-asset subject of this white paper may be held or claimed by third parties having no connection with the crypto-asset itself, and claims of that kind have been asserted, including demands addressed to trading venues. The crypto-asset cannot be rebranded, as its name and ticker are recorded on the underlying network, and no person has been identified as able to defend, license or settle such claims on behalf of holders. Trading venues and other service providers may respond to such claims by restricting the display, promotion or availability of the crypto-asset. The status and merits of any such claims have not been determined.

### **1.4 Project implementation-related risks**

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

The principal project implementation-related risks for the crypto-asset are as follows:

1. Key-contributor and concentration risk: The continued development, maintenance, and upgrading of the crypto-asset and the related network may depend on a limited number of core protocol contributors, client-software development teams, and supporting organisations such as foundations. The departure, incapacity, loss of funding, or strategic misalignment of such contributors or organisations, or an over-reliance on a dominant client implementation, may delay, fragment, or otherwise adversely affect the implementation and ongoing evolution of the crypto-asset.
2. Timeline and milestone risk: Protocol upgrades, feature releases, scaling improvements, or other initiatives set out in any public roadmap or technical documentation may not be delivered as announced, may be delayed, or may be abandoned. Such delays or changes can undermine market confidence and affect the adoption, use, or perceived value of the crypto-asset.
3. Delivery risk: Even where an upgrade or feature is delivered as planned, it may not perform as intended, may introduce unintended effects, or may be scaled back during or after deployment, which may limit the practical functionality or expected benefits of the crypto-asset.

### **1.5 Technology-related risks**

As this white paper relates to admission to trading of the crypto-asset, the following risks concern the underlying distributed ledger technology (DLT), its supporting infrastructure, and related

technical dependencies. Failures or vulnerabilities in these systems may affect the availability, integrity, or transferability of the crypto-asset.

### 1. Blockchain dependency risk

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

### 2. Program, mint configuration and token-infrastructure risk

The crypto-asset subject of this white paper is issued on the Solana network and relies on that network's shared token-program infrastructure rather than on a project-specific smart contract governing the token itself. Its token-specific parameters are recorded in the associated mint account, including the configuration of administrative authorities such as the mint authority and, where applicable, the freeze authority. Incorrect configuration or compromise of any active authority may affect the supply, transferability, or availability of the crypto-asset. The crypto-asset also depends on the correct operation of the shared Solana token program and of any further on-chain programs through which it is traded or held. Coding errors, security vulnerabilities, misconfiguration, or unauthorised changes affecting such programs may result in failed or unintended transactions, disruption of functionality, or loss of assets. Undetected vulnerabilities may persist even after external audits, and where a relevant program remains upgradeable, changes introduced through its upgrade authority may alter its behaviour or introduce new vulnerabilities.

### 3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

### 4. Network security risks

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



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

#### 5. Bridge and interoperability risk

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

#### 6. Forking and protocol-upgrade risk

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

#### 7. Economic-layer and abstraction risk

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

#### 8. Spam and network-efficiency risk

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

#### 9. Front-end and access-interface risk

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

#### 10. Decentralisation claim risk

While the technical infrastructure may appear distributed, the actual governance or economic control of the project may lie with a small set of actors. This disconnect between marketing claims

and structural reality can lead to regulatory scrutiny, reputational damage, or legal uncertainty – especially if the project is presented as ‘community-governed’ without substantiation.

## **I.6 Mitigation measures**

None.

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

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

#### **S.1 Name**

Crypto Risk Metrics GmbH

#### **S.2 Relevant legal entity identifier**

39120077M9TG001FE242

#### **S.3 Name of the crypto-asset**

Peanut the Squirrel

#### **S.4 Consensus Mechanism**

The crypto-asset that is the subject of this white paper is available on the Solana network.

The following applies to Solana:

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

#### Core Concepts

##### 1. Proof-of-History (PoH):

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

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

##### 2. Proof-of-Stake (PoS):

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

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

## Consensus Process

### 1. Transaction Validation:

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

### 2. PoH Sequence Generation:

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

### 3. Block Production:

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

### 4. Consensus and Finalisation:

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

## Security and Economic Incentives

### 1. Incentives for Validators:

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

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

## 2. Security:

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

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

## 3. Economic Penalties:

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

## **S.5 Incentive Mechanisms and Applicable Fees**

The crypto-asset that is the subject of this white paper is available on the Solana network.

The following applies to Solana:

### 1. Validators:

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

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

### 2. Delegators:

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

### 3. Economic Security:

Solana staking documentation notes slashing as a possible future mechanism for intentional malicious conduct, but states that slashing is not implemented in the protocol today. Economic

alignment instead currently arises primarily from staking participation, validator performance incentives, and the opportunity cost of locking capital in staking positions.

#### Fees Applicable on the Solana Blockchain

##### 1. Transaction Fees:

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

##### 2. Rent Fees:

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

##### 3. Program Execution Costs:

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

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

2024-05-28

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

2025-05-28

## **S.8 Energy consumption**

131.24154 kWh/a

## **S.9 Energy consumption sources and methodologies**

The energy consumption of this asset is aggregated across multiple components: To determine the energy consumption of a token, the energy consumption of the network Solana is calculated first. For the energy consumption of the token, a fraction of the energy consumption of the network is attributed to the token, which is determined based on the activity of the crypto-asset within the network. When calculating the energy consumption, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used - if available - to determine all implementations of the asset in scope. The mappings are updated regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

## **S.10 Renewable energy consumption**

38.5831139958 %

## **S.11 Energy intensity**

0.00000 kWh

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

0.00000 tCO<sub>2</sub>e/a

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

0.04368 tCO<sub>2</sub>e/a

## **S.14 GHG intensity**

0.00000 kgCO<sub>2</sub>e

## **S.15 Key energy sources and methodologies**

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

Ember (2025); Energy Institute, Statistical Review of World Energy (2024), with major processing by Our World in Data. "Share of electricity generated by renewables - Ember and Energy Institute" [dataset]. Underlying sources: Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: <https://ourworldindata.org/grapher/share-electricity-renewables>

## **S.16 Key GHG sources and methodologies**

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

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

