CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG 4GX02L80B

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 10
A.1 Name 10
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 11
A.13 Business activity 11
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 14
C.1 Name 14
C.2 Legal form 14
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 15
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 15
Part D – Information about the crypto-asset project 15
D.1 Crypto-asset project name 15
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 16
D.6 Utility Token Classification 16
D.7 Key Features of Goods/Services for Utility Token Projects 16
D.8 Plans for the token 16
D.9 Resource allocation 18
D.10 Planned use of Collected funds or crypto-Assets 19
Part E – Information about the offer to the public of crypto-assets or their admission to trading 19
E.1 Public offering or admission to trading 19
E.2 Reasons for public offer or admission to trading 19
E.3 Fundraising target 19
E.4 Minimum subscription goals 19
E.5 Maximum subscription goals 20
E.6 Oversubscription acceptance 20
E.7 Oversubscription allocation 20
E.8 Issue price 20
E.9 Official currency or any other crypto-assets determining the issue price 20
E.10 Subscription fee 20
E.11 Offer price determination method 20
E.12 Total number of offered/traded crypto-assets 20
E.13 Targeted holders 20
E.14 Holder restrictions 20
E.15 Reimbursement notice 21
E.16 Refund mechanism 21
E.17 Refund timeline 21
E.18 Offer phases 21
E.19 Early purchase discount 21
E.20 Time-limited offer 21
E.21 Subscription period beginning 21
E.22 Subscription period end 21
E.23 Safeguarding arrangements for offered funds/crypto- Assets 21
E.24 Payment methods for crypto-asset purchase 21
E.25 Value transfer methods for reimbursement 21
E.26 Right of withdrawal 22
E.27 Transfer of purchased crypto-assets 22

E.28 Transfer time schedule 22
E.29 Purchaser's technical requirements 22
E.30 Crypto-asset service provider (CASP) name 22
E.31 CASP identifier 22
E.32 Placement form 22
E.33 Trading platforms name 22
E.34 Trading platforms Market identifier code (MIC) 22
E.35 Trading platforms access 22
E.36 Involved costs 22
E.37 Offer expenses 23
E.38 Conflicts of interest 23
E.39 Applicable law 23
E.40 Competent court 23
Part F – Information about the crypto-assets 23
F.1 Crypto-asset type 23
F.2 Crypto-asset functionality 24
F.3 Planned application of functionalities 24
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 25
F.4 Type of crypto-asset white paper 25
F.5 The type of submission 25
F.6 Crypto-asset characteristics 25
F.7 Commercial name or trading name 25
F.8 Website of the issuer 26
F.9 Starting date of offer to the public or admission to trading 26
F.10 Publication date 26
F.11 Any other services provided by the issuer 26
F.12 Language or languages of the crypto-asset white paper 26
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 26
F.14 Functionally fungible group digital token identifier 26
F.15 Voluntary data flag 26
F.16 Personal data flag 26
F.17 LEI eligibility 26
F.18 Home Member State 26
F.19 Host Member States 26

Part G – Information on the rights and obligations attached to the crypto-assets 26
G.1 Purchaser rights and obligations 26
G.2 Exercise of rights and obligations 27
G.3 Conditions for modifications of rights and obligations 27
G.4 Future public offers 27
G.5 Issuer retained crypto-assets 27
G.6 Utility token classification 28
G.7 Key features of goods/services of utility tokens 28
G.8 Utility tokens redemption 28
G.9 Non-trading request 28
G.10 Crypto-assets purchase or sale modalities 28
G.11 Crypto-assets transfer restrictions 28
G.12 Supply adjustment protocols 28
G.13 Supply adjustment mechanisms 28
G.14 Token value protection schemes 28
G.15 Token value protection schemes description 28
G.16 Compensation schemes 29
G.17 Compensation schemes description 29
G.18 Applicable law 29
G.19 Competent court 29
Part H – information on the underlying technology 29
H.1 Distributed ledger technology (DTL) 29
H.2 Protocols and technical standards 29
H.3 Technology used 32
H.4 Consensus mechanism 32
H.5 Incentive mechanisms and applicable fees 34
H.6 Use of distributed ledger technology 36
H.7 DLT functionality description 36
H.8 Audit 36
H.9 Audit outcome 36
Part I – Information on risks 36
I.1 Offer-related risks 36
I.2 Issuer-related risks 38
I.3 Crypto-assets-related risks 39
I.4 Project implementation-related risks 41
I.5 Technology-related risks 42

I.6 Mitigation measures 44

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts 44

J.1 Adverse impacts on climate and other environment-related adverse impacts 44

S.1 Name 44

S.2 Relevant legal entity identifier 44

S.3 Name of the crypto-asset 44

S.4 Consensus Mechanism 44

S.5 Incentive Mechanisms and Applicable Fees 46

S.6 Beginning of the period to which the disclosure relates 48

S.7 End of the period to which the disclosure relates 48

S.8 Energy consumption 48

S.9 Energy consumption sources and methodologies 48

S.10 Renewable energy consumption 48

S.11 Energy intensity 48

S.12 Scope 1 DLT GHG emissions – Controlled 48

S.13 Scope 2 DLT GHG emissions – Purchased 48

S.14 GHG intensity 48

S.15 Key energy sources and methodologies 48

S.16 Key GHG sources and methodologies 49

01. Date of notification

This white paper was notified on 2026-04-24.

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 HNT referred to in this white paper is a crypto-asset other than EMTs and ARTs and is deployed on the Solana and Helium networks, according to the DTI FFG shown in section F. 14, as of 2026-04-22. The maximum supply of the crypto-asset is 223,000,000 tokens. The first activity of the Solana network can be viewed on 2024-07-18 (signature hash: E7fEyHWfPZiGpHENsvPps7bDdZp1LUvxrN7yoLJzWsSQ9QoHbw5Po1jfGjV7d2EbNnE1xV3kbXHrq9bqUCpKcWj, source: https://solscan.io/tx/ E7fEyHWfPZiGpHENsvPps7bDdZp1LUvxrN7yoLJzWsSQ9QoHbw5Po1jfGjV7d2EbNnE1xV3kbXHrq9bqUCpKcWj accessed 2026-04-22). Following the migration of the Helium Network to Solana on 18 April 2023, the legacy Helium blockchain ceased operating, and no further on-chain activity is recorded for that legacy network.

The Helium Network is a decentralised wireless infrastructure project designed to provide connectivity for Internet of Things devices and mobile devices through a distributed network of participant-operated hotspots. The project includes an IoT network based on LoRaWAN and a mobile network providing 5G and Wi-Fi connectivity. Hotspot operators deploy compatible hardware that provides wireless coverage and relays network traffic, while the protocol uses a Proof-of-Coverage mechanism to verify that participating hotspots are located as claimed and are providing the reported wireless service. The project migrated from its original blockchain to the Solana blockchain in April 2023, and network activity is now recorded through that execution environment.

The crypto-asset HNT is the native crypto-asset of the Helium ecosystem and is used to support its protocol-level incentive and operational model. HNT is used to reward eligible participants that provide wireless coverage and handle data traffic. It is also used to create Data Credits through a burn mechanism, with Data Credits used to pay for data transmission and certain transaction-related costs within the network. HNT may also be used in governance through token locking arrangements that provide voting power in relation to network decisions. Based on the information provided, the crypto-asset follows a burn-and-mint equilibrium model and a scheduled issuance reduction mechanism.

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

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

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

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

Crypto Risk Metrics GmbH is seeking admission to trading on the Payward Global Solutions LTD (“Kraken”) platform in the European Union in accordance with Article 5 of Regulation (EU) 2023/1114

of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. The admission to trading is not accompanied by a public offer of the crypto-asset.

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

DE-HH

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

Nova Labs Inc. (also operating under the name "Helium Systems, Inc.", formerly known as Skynet Phase 1 Inc.)

B.3 Legal form

The legal form of Nova Labs Inc. is XTIQ, which corresponds to "Corporation".

B.4 Registered address

The registered address of the Nova Labs Inc. is 160 Greentree Dr Ste 101, Dover, Kent, DE, 19904,

United States,

US-DE

B.5 Head office

The head office of Nova Labs Inc. is 2261 Market Street, Suite 10194, San Francisco, CA 94114,

United States,

US-CA

B.6 Registration date

Nova Labs Inc. was registered on 2023-05-28.

B.7 Legal entity identifier

Nova Labs Inc. has no Legal Entity Identifier (LEI).

B.8 Another identifier required pursuant to applicable national law

Delaware file number: 5341383

B.9 Parent company

No parent company of Nova Labs Inc. can be identified.

B.10 Members of the management body

Identity	Function	Business Address
Amir Haleem	CEO	2261 Market Street, Suite 10194, San Francisco, CA 94114, United States

B.11 Business activity

Nova Labs is a technology company focused on decentralised wireless network infrastructure. Its business activities have included the development of software protocols, blockchain-based network coordination mechanisms, Hotspot and wireless-device related products, and services connected to low-power and cellular data connectivity. Nova Labs has also been involved in the development and promotion of the Helium Network, including network infrastructure, and related connectivity services.

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: "Helium", Short Name: "HNT" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-22).

D.2 Crypto-assets name

Long Name: "Helium" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-04-22).

D.3 Abbreviation

Short Name: "HNT" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-22).

D.4 Crypto-asset project description

According to public information published in the Helium documentation, the Helium project is a decentralised wireless network project designed to support device connectivity and data transfer through community-operated physical infrastructure. The project developed as a decentralised physical infrastructure network and is intended to provide wireless coverage through a distributed model in which independent participants deploy and operate network hardware. The Helium ecosystem supports connectivity for low-power Internet of Things devices through a LoRaWAN-based network and also supports a mobile connectivity framework involving 5G and Wi-Fi based services. Its design has included technical mechanisms such as community-operated Hotspots, cryptographic verification of wireless coverage through Proof-of-Coverage, and a token-based usage model involving the conversion of HNT into Data Credits for payment of network usage fees. Following the migration of the Helium network from its original blockchain infrastructure to the Solana blockchain in April 2023, the project has continued to operate through a structure combining wireless-network functionality with Solana-based token and asset infrastructure. The protocol further supports technical processes relating to hotspot representation, reward distribution, off-chain oracle based calculations, and continuing development concerning network operations, infrastructure deployment, and application support. The HNT crypto-asset functions as a core technical element within this broader framework. It is used within the network's token model in connection with rewards, and may also be burned to create Data Credits used for data transmission and other network-related usage.

The project does not involve the granting of ownership, profit-participation rights, or legal claims against the Helium protocol or its contributors. Instead, it centres on the creation of a technical environment in which the HNT crypto-asset may serve as an operational input for certain protocol processes. The long-term evolution of the Helium system, including the scope of available features, the validator-participation framework, committee- or leader-selection mechanisms, and the

operational continuity of the infrastructure, may vary based on technical, economic, and regulatory considerations. All future developments remain subject to change.

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

Name of person	Type of person	Business address of person	Domicile of company
Abhay Kumar	Other person involved in implementation	Cannot be found	United States
Amir Haleem	Other person involved in implementation	Cannot be found	United States
Decentralized Wireless Foundation, Inc.	Other person involved in implementation	140 E Broadway Ave, Ste 25, 83001 Jackson, US-WY	United States
Nova Labs Inc. (Helium Systems, Inc.)	Other person involved in implementation	160 Greentree Dr Ste 101, Dover, Kent, DE, 19904	United States

D.6 Utility Token Classification

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

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

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

D.8 Plans for the token

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

There is no formally published multi-year roadmap for the HNT crypto-asset. Based on public information (sources: https://docs.helium.com/, https://github.com/helium/HIP, accessed 2026-04-22), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Helium protocol and the role of the HNT crypto-asset.

Past milestones:

- Founding of Helium (2013): Helium was founded in San Francisco by Amir Haleem.

- Early Funding Rounds (2011-2016): The project raised capital through a USD 10 million debt round in 2011, a USD 2.85 million seed round in 2014, a USD 16 million Series A round in 2014, and a USD 20 million Series B round in 2016.

- Series C Funding and Network Launch (29 July 2019): Helium raised USD 15 million in Series C funding in June 2019, and the first HNT was emitted on 29 July 2019, marking the launch of the Helium Network.

- HIP-20 Approval and Additional Funding (2021-2022): The community approved HIP-20 establishing a two-year halving schedule for HNT emissions.

- Solana Migration Proposal (August 2022): HIP-70 was proposed to migrate the Helium blockchain to Solana and to move certain network functions, including Proof-of-Coverage and Data Transfer Accounting, to oracle-based mechanisms.

- Leadership Change and Strata Acquisition (November 2022): Abhay Kumar was appointed CEO of the Helium Foundation, and the Helium Foundation acquired The Strata Protocol in connection with the planned Solana migration.

- Solana Migration Completion (18 April 2023): Helium completed its migration from its custom Layer 1 blockchain to the Solana blockchain.

- Sixth Emissions Year (1 August 2024): The network entered its sixth year of emissions with a target annual HNT emission of 15,000,000 HNT.

- Return to HNT-Based Rewards (15 January 2025): Under HIP-138, the network returned to HNT-based rewards by phasing out IOT and MOBILE subnetwork token rewards.

- HNT Halving (1 August 2025): The annual HNT emission target is scheduled to halve from 15,000,000 HNT to 7,500,000 HNT.

- HIP-148 Governance Vote (10 October 2025): HIP-148 was voted on to reallocate Mobile Mapping rewards and simplify the MOBILE tokenomics framework.

Future milestones:

- Global Expansion Phase (2026): The year 2026 has been described as a phase of broader network expansion following the prior development phase.

- Infrastructure Scaling (Date not specified): Future plans include further integration of 5G coverage, onboarding additional hotspot operators, and expanding partnerships with telecom providers.

- User Experience Improvements (Date not specified): Future development includes a planned "Welcome Pack" system and integration with email-login solutions such as Privy to simplify onboarding for mainstream users.

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

D.9 Resource allocation

According to publicly referenced information, the business associated with the Helium project, now operating as Nova Labs, Inc. (also known as Helium Systems, Inc.), is reported to have first raised approximately USD 10,000,000 in conventional debt financing in or around May 2011, with Agile Equity referenced as lead investor. This financing appears to relate to earlier non-blockchain business activities and not to the HNT crypto-asset or the later blockchain-based Helium Network. Public sources further indicate that, in or around April 2014, the company completed a seed financing round in the amount of approximately USD 2,850,000, involving investors identified in public materials as including SV Angel, Slow Ventures, FirstMark, and Digital Garage. Further public reporting indicates that, in or around October 2014, a Series A financing round followed in the amount of approximately USD 16,000,000, with participation reported from Khosla Ventures, SV Angel, Slow Ventures, FirstMark, and Digital Garage.

According to publicly referenced information, Nova Labs, Inc. subsequently completed a Series B round in or around April 2016 in the amount of approximately USD 20,000,000. Public materials referenced by third parties describe participation in that round from Google Ventures (GV), Khosla Ventures, Munich Re Ventures, and FirstMark. Public sources further indicate that, in or around June 2019, the company completed a Series C financing round in the amount of approximately USD 15,000,000, with investors reported as including Union Square Ventures, Multicoin Capital, Khosla Ventures, Google Ventures (GV), Munich Re Ventures, and FirstMark.

Third-party reporting further describes a significant token-linked financing round in or around August 2021, when approximately USD 111,000,000 is reported to have been raised through a sale of HNT tokens. Publicly referenced materials identify Andreessen Horowitz (a16z) as lead investor in that transaction, with additional participation reported from Multicoin Capital, Ribbit Capital, Alameda Research, and 10T Holdings. Thereafter, according to publicly referenced information, Nova Labs, Inc. completed a further Series D financing round in or around February 2022 in the amount of approximately USD 200,000,000 at a reported valuation of approximately USD

1,200,000,000. Public sources identify Tiger Global Management, Andreessen Horowitz (a16z), and Munich Re Ventures as lead participants, with additional investors reported as including Seven Seven Six, Google Ventures (GV), Multicoin Capital, Pantera Capital, Ribbit Capital, Khosla Ventures, and FTX Ventures.

Public sources commonly describe the Helium or Nova Labs project as having raised approximately USD 370,000,000 across seven funding rounds. However, the individual round amounts frequently cited in public materials, if aggregated, produce a figure of approximately USD 374,850,000. Accordingly, there appears to be some inconsistency in third-party reporting as to whether all financing events, including the earlier conventional debt financing or token sale proceeds, are included in the commonly cited cumulative total.

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

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

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The maximum supply of the crypto-asset is set at 223,000,000 tokens. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

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

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

E.36 Involved costs

The costs involved in accessing the trading platform depend on the specific fee structure and terms of the respective crypto-asset service provider. These may include trading fees, deposit or

withdrawal charges, and network-related gas fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

claims to its holders, and therefore remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

The HNT token is designed to support technical and governance-related functions within the Helium protocol environment. Since 18 April 2023, HNT has operated as an SPL-compatible token on the Solana blockchain. Within the Helium ecosystem, HNT is used to support network participation and protocol operation in several ways. Holders and network participants may receive HNT in connection with the provision of wireless coverage and the operation of Hotspots within the Helium network. HNT may also be burned in order to generate Data Credits, which are used within the protocol environment to pay for data transmission and certain transaction-related costs. In addition, holders may lock HNT to obtain veHNT, which may be used to participate in governance processes within the Helium DAO, including voting on protocol-related matters and the direction of rewards across supported subnetworks, in accordance with the applicable governance framework.

The HNT token also forms part of the protocol's broader issuance, burn, and reward-balancing design. According to the project documentation, the protocol operates with a capped maximum supply of 223,000,000 HNT and a programmed emission model based on recurring halving events. HNT issuance is used to reward eligible network participants, while HNT may be permanently burned in order to create Data Credits used for network consumption. Because Data Credits are generated through the destruction of HNT and are not convertible back into HNT, network usage may contribute to a reduction in the amount of HNT remaining in circulation.

The protocol documentation further describes a burn-and-mint equilibrium mechanism under which a limited portion of previously burned HNT may be re-minted for reward distribution. This re-minting is subject to protocol-defined limitations, including caps intended to restrict the amount of HNT that may be reintroduced over a given period, and is described as operating without increasing the maximum supply beyond the stated cap. The protocol also describes a calculation method intended to smooth the amount of HNT re-minted over time in order to reduce abrupt fluctuations in reward distribution.

As a result, although the total maximum supply of HNT is described as fixed, the effective circulating supply may vary over time depending on the interaction between scheduled token issuance, the volume of HNT burned for the generation of Data Credits, and the operation of the protocol's capped re-minting mechanism. Accordingly, the amount of HNT effectively available in circulation may increase more slowly, remain relatively stable, or decrease over time depending on the level of network usage and the application of the relevant protocol rules.

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

F.3 Planned application of functionalities

Future milestones:

- Global Expansion Phase (2026): The year 2026 has been described as a phase of broader network expansion following the prior development phase.

- Infrastructure Scaling (Date not specified): Future plans include further integration of 5G coverage, onboarding additional hotspot operators, and expanding partnerships with telecom providers.

- User Experience Improvements (Date not specified): Future development includes a planned "Welcome Pack" system and integration with email-login solutions such as Privy to simplify onboarding for mainstream users.

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

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs and is currently available on the Solana network, having previously been available on the Helium network, which is no longer operational. The crypto-asset is fungible up to 8 digits after the decimal point on Solana and is no longer available on the discontinued Helium blockchain. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics such as supply, demand, and liquidity in secondary markets.

F.7 Commercial name or trading name

Long Name: "Helium" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-04-22).

F.8 Website of the issuer

https://www.helium.com/

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

2026-05-29

F.10 Publication date

2026-05-29

F.11 Any other services provided by the issuer

No such services are currently known to be provided by the issuer. However, it cannot be excluded that additional services exist or may be offered in the future outside the scope of Regulation (EU) 2023/1114.

F.12 Language or languages of the crypto-asset white paper

EN

F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates

LPPHF6K4C, VS93QW822

F.14 Functionally fungible group digital token identifier

4GX02L80B

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-04-21).

G.5 Issuer retained crypto-assets

No HNT crypto-assets were allocated to the issuer through a pre-mine or initial issuer allocation at the launch of the Helium Network. Based on the information reviewed, HNT was emitted through the protocol's issuance mechanism rather than pre-allocated as a fixed amount to Nova Labs or another identified issuer.

The Helium Network historically included a separate mechanism known as the Helium Security Token ("HST"). HST was not the same asset as HNT. Based on publicly available information, HST entitled its holders to receive a share of ongoing HNT emissions. Available materials refer to HST holders receiving a portion of newly emitted HNT, including historical references to up to 35% of newly created HNT and later references to 30% decreasing over time to 15%. Helium governance materials describe HST holders as investors in, and early employees of, Nova Labs, Inc. Publicly available information also indicates that Nova Labs retained approximately 2,000 HST out of a total of 10,300 HST.

For the purposes of this section, issuer-retained crypto-assets are disclosed as 0 HNT, because no verifiable fixed issuer-retained HNT allocation or issuer-controlled HNT wallet balance has been identified. This does not exclude that Nova Labs, its investors, employees, or other related parties may have received HNT over time through HST-based emission rights.

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 2026-04-22.

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

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 223,000,000 units according to public information (Source: https://docs.helium.com/tokens/hnt-token, 2026-04-22). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

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 limiting the need for a global transaction mempool.

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

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

2. Address and Cryptographic Standards

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

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

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

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

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

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

3. Networking and Data Transmission Standards

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

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

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

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

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

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

4. Token and Program Standards (Solana Program Library)

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

Within this framework:

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

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

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

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

5. Protocol Development and Improvement Standards

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

The following applies to Helium:

Helium initially operated on its own custom Layer 1 blockchain, which was discontinued following the project's migration to the Solana network on 18 April 2023.

H.3 Technology used

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

The following applies to Solana:

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

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

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

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

Security Protocols for Asset Custody and Transactions:

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

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

The following applies to Helium:

Helium initially operated on its own custom Layer 1 blockchain, which was discontinued following the project's migration to the Solana network on 18 April 2023.

H.4 Consensus mechanism

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

The following applies to Solana:

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

Core Concepts

1. Proof-of-History (PoH):

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

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

2. Proof-of-Stake (PoS):

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

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

3. Block Production:

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

4. Consensus and Finalisation:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

The following applies to Helium:

Helium initially operated on its own custom Layer 1 blockchain, which was discontinued following the project's migration to the Solana network on 18 April 2023.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

2. Rent Fees:

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

3. Program Execution Costs:

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

The following applies to Helium:

Helium initially operated on its own custom Layer 1 blockchain, which was discontinued following the project's migration to the Solana network on 18 April 2023.

H.6 Use of distributed ledger technology

No – 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.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

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

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

Insolvency of counterparties: If a counterparty involved in holding, routing, or settling the crypto-asset becomes insolvent, enters restructuring, or is otherwise subject to resolution measures, assets held or processed by that counterparty may be frozen, become temporarily unavailable, or

be recoverable only in part or not at all, which can result in losses for clients whose positions were maintained through that counterparty. This risk applies in particular where client assets are held on an omnibus basis or where segregation is not fully recognised in the counterparty's jurisdiction.

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

Delays, failures, or changes in the implementation of the project as outlined in its public roadmap or technical documentation may negatively impact the perceived credibility or usability of the crypto-

asset. This includes risks related to project governance, resource allocation, technical delivery, and team continuity.

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

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

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the crypto-asset

Helium

S.4 Consensus Mechanism

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

The following applies to Solana:

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

Core Concepts

1. Proof-of-History (PoH):

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

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

2. Proof-of-Stake (PoS):

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

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

3. Block Production:

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

4. Consensus and Finalisation:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

The following applies to Helium:

Helium initially operated on its own custom Layer 1 blockchain, which was discontinued following the project's migration to the Solana network on 18 April 2023.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is implemented on the Solana network and was previously implemented on the Helium network, which is no longer operational, following the standards described below.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

2. Rent Fees:

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

3. Program Execution Costs:

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

The following applies to Helium:

Helium initially operated on its own custom Layer 1 blockchain, which was discontinued following the project’s migration to the Solana network on 18 April 2023.

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

2025-04-22

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

2026-04-22

S.8 Energy consumption

153.06214 kWh/a

S.9 Energy consumption sources and methodologies

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

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

S.10 Renewable energy consumption

38.5831139958 %

S.11 Energy intensity

0.00000 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.05094 tCO2e/a

S.14 GHG intensity

0.00000 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are determined using public information sites, open-source and in-house-developed crawlers. Where no

information is available on the geographic distribution of nodes, comparable reference networks are used, taking into account similarities in incentivisation structure and consensus mechanism. This geographic information is then combined with publicly available data from Our World in Data. The resulting intensity is calculated as the marginal energy consumption with respect to one additional transaction.

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

S.16 Key GHG sources and methodologies

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

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.