

**White paper drafted under the  
European Markets in Crypto-  
Assets Regulation (EU)  
2023/1114 for FFG NT91TJWNC**

## Preamble

### 00. Table of Content

Preamble	2
01. Date of notification	8
02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	8
03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	8
04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114	8
05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114	8
06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114	8
Summary	8
07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114	8
08. Characteristics of the crypto-asset	8
09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	9
10. Key information about the offer to the public or admission to trading	9
Part A – Information about the offeror or the person seeking admission to trading	9
A.1 Name	9
A.2 Legal form	10
A.3 Registered address	10
A.4 Head office	10
A.5 Registration date	10
A.6 Legal entity identifier	10
A.7 Another identifier required pursuant to applicable national law	10
A.8 Contact telephone number	10
A.9 E-mail address	10
A.10 Response time (Days)	10
A.11 Parent company	10
A.12 Members of the management body	10
A.13 Business activity	10
A.14 Parent company business activity	10
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	12
B.6 Registration date	12
B.7 Legal entity identifier	12
B.8 Another identifier required pursuant to applicable national law	12
B.9 Parent company	12
B.10 Members of the management body	13
B.11 Business activity	13
B.12 Parent company business activity	13
Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	13
C.1 Name	13
C.2 Legal form	13
C.3 Registered address	13
C.4 Head office	13
C.5 Registration date	13
C.6 Legal entity identifier	13
C.7 Another identifier required pursuant to applicable national law	14
C.8 Parent company	14
C.9 Reason for crypto-Asset white paper Preparation	14
C.10 Members of the Management body	14
C.11 Operator business activity	14
C.12 Parent company business activity	14
C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	14
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	14
Part D – Information about the crypto-asset project	14
D.1 Crypto-asset project name	14
D.2 Crypto-assets name	14
D.3 Abbreviation	14

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

E.28 Transfer time schedule	20
E.29 Purchaser's technical requirements	20
E.30 Crypto-asset service provider (CASP) name	21
E.31 CASP identifier	21
E.32 Placement form	21
E.33 Trading platforms name	21
E.34 Trading platforms Market identifier code (MIC)	21
E.35 Trading platforms access	21
E.36 Involved costs	21
E.37 Offer expenses	21
E.38 Conflicts of interest	21
E.39 Applicable law	22
E.40 Competent court	22
Part F – Information about the crypto-assets	22
F.1 Crypto-asset type	22
F.2 Crypto-asset functionality	22
F.3 Planned application of functionalities	23
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	23
F.4 Type of crypto-asset white paper	23
F.5 The type of submission	23
F.6 Crypto-asset characteristics	23
F.7 Commercial name or trading name	24
F.8 Website of the issuer	24
F.9 Starting date of offer to the public or admission to trading	24
F.10 Publication date	24
F.11 Any other services provided by the issuer	24
F.12 Language or languages of the crypto-asset white paper	24
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	24
F.14 Functionally fungible group digital token identifier	24
F.15 Voluntary data flag	24
F.16 Personal data flag	24
F.17 LEI eligibility	24
F.18 Home Member State	24
F.19 Host Member States	25

Part G – Information on the rights and obligations attached to the crypto-assets	25
G.1 Purchaser rights and obligations	25
G.2 Exercise of rights and obligations	25
G.3 Conditions for modifications of rights and obligations	25
G.4 Future public offers	25
G.5 Issuer retained crypto-assets	26
G.6 Utility token classification	26
G.7 Key features of goods/services of utility tokens	26
G.8 Utility tokens redemption	26
G.9 Non-trading request	26
G.10 Crypto-assets purchase or sale modalities	26
G.11 Crypto-assets transfer restrictions	26
G.12 Supply adjustment protocols	26
G.13 Supply adjustment mechanisms	27
G.14 Token value protection schemes	27
G.15 Token value protection schemes description	27
G.16 Compensation schemes	27
G.17 Compensation schemes description	27
G.18 Applicable law	27
G.19 Competent court	27
Part H – information on the underlying technology	27
H.1 Distributed ledger technology (DTL)	27
H.2 Protocols and technical standards	27
H.3 Technology used	28
H.4 Consensus mechanism	29
H.5 Incentive mechanisms and applicable fees	31
H.6 Use of distributed ledger technology	32
H.7 DLT functionality description	32
H.8 Audit	33
H.9 Audit outcome	33
Part I – Information on risks	33
I.1 Offer-related risks	33
I.2 Issuer-related risks	35
I.3 Crypto-assets-related risks	36
I.4 Project implementation-related risks	38
I.5 Technology-related risks	38

I.6 Mitigation measures	40
Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts	41
J.1 Adverse impacts on climate and other environment-related adverse impacts	41
S.1 Name	41
S.2 Relevant legal entity identifier	41
S.3 Name of the cryptoasset	41
S.4 Consensus Mechanism	41
S.5 Incentive Mechanisms and Applicable Fees	43
S.6 Beginning of the period to which the disclosure relates	44
S.7 End of the period to which the disclosure relates	44
S.8 Energy consumption	44
S.9 Energy consumption sources and methodologies	44
S.10 Renewable energy consumption	45
S.11 Energy intensity	45
S.12 Scope 1 DLT GHG emissions – Controlled	45
S.13 Scope 2 DLT GHG emissions – Purchased	45
S.14 GHG intensity	45
S.15 Key energy sources and methodologies	45
S.16 Key GHG sources and methodologies	45

## **01. Date of notification**

2025-12-15

## **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 deBridge (DBR) referred to in this white paper is a crypto-asset other than EMTs and ARTs, and is issued on the Solana network as of 2025-12-08 and according to DTI FFG shown in F.14. The maximum supply of the crypto-asset is fixed at 10,000,000,000 units. The first activity in Solana can be viewed on 2024-07-24 (transaction hash: 47VERsnW4nyRf76TtGHP8tbiD3kELv7fpFnWHAi4ENCxePypkKGuwkNLTwHH24PXbebDd2BnL3eDDPEFBjxVgUWk, source <https://solscan.io/tx/47VERsnW4nyRf76TtGHP8tbiD3kELv7fpFnWHAi4ENCxePypkKGuwkNLTwHH24PXbebDd2BnL3eDDPEFBjxVgUWk>, accessed 2025-12-08).

DeBridge is a cross-chain interoperability protocol that enables users and applications to transfer liquidity and data between supported blockchains through non-custodial smart-contract infrastructure. The DBR crypto-asset serves as the native governance instrument within this ecosystem: holders may use DBR to participate in protocol governance, influence parameter settings, and pay for computing resources provided by validators. DBR may also be staked once the delegated staking and slashing modules are activated.

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

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

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

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

Crypto Risk Metrics GmbH is seeking admission to trading on any Crypto Asset Service Provider platform in the European Union in accordance to 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. In accordance to Article 5(4), this crypto-asset white paper may be used by entities admitting the token to trading after Crypto Risk Metrics GmbH as the person responsible for drawing up such white paper has given its consent to its use in writing to the respective Crypto Asset Service Provider.

## **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 DE-HH, Lange Reihe 73, 20099 Hamburg, Germany.

## A.4 Head office

Crypto Risk Metrics GmbH has no head office.

## A.5 Registration date

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

## A.6 Legal entity identifier

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

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

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

## A.8 Contact telephone number

+4915144974120

## A.9 E-mail address

info@crypto-risk-metrics.com

## A.10 Response time (Days)

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

## A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

## A.12 Members of the management body

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

## A.13 Business activity

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

## A.14 Parent company business activity

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

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

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

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

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

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

2024 (unaudited): negative EUR 50.891,81

2023 (unaudited): negative EUR 27.665,32

2022: EUR 104.283,00.

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

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

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

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

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

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

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

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

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

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

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

### **B.2 Name**

deBridge Foundation

### **B.3 Legal form**

The legal form of deBridge Foundation is MPUG, which corresponds to "Limited Liability Company".

### **B.4. Registered address**

The registered address of deBridge Foundation is KY-05, George Town Financial Center, Suite 303, 90 Fort Street, George Town, Grand Cayman, KY1-1104, Cayman Islands

### **B.5 Head office**

The head office of Definitive Finance Inc. is the same as its registered address.

### **B.6 Registration date**

Could not be found while drafting this white paper (2025-12-08).

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

DeBridge Foundation has no Legal Entity Identifier (LEI).

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

Could not be found while drafting this white paper (2025-12-08).

### **B.9 Parent company**

No parent company of deBridge Foundation can be identified.

## B.10 Members of the management body

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

## B.11 Business activity

The deBridge Foundation oversees and advances the development, governance progression, and long-term sustainability of the deBridge protocol. Its activities encompass maintaining and enhancing the protocol's technical infrastructure, administering grants and incentive programs to support ecosystem growth, and steering the transition toward greater decentralization. The Foundation manages the DBR token treasury and reserve mechanisms, including allocation of protocol earnings and liquidity-support strategies, and acts as the responsible entity for conducting airdrop distributions. All activities are carried out for the benefit of the deBridge DAO, its contributors, partners, and the wider community.

## B.12 Parent company business activity

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

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

### C.1 Name

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

### 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: "deBridge", short name: "DBR" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2025-04-30).

### **D.2 Crypto-assets name**

Long name: "deBridge" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2025-04-30).

### **D.3 Abbreviation**

Short name: "DBR" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2025-04-30).

### **D.4 Crypto-asset project description**

According to public information (source: <https://debridge.com/>, accessed 2025-12-08), the deBridge project is a crypto-asset initiative concerned with the development and operation of the deBridge interoperability infrastructure, a software system designed to facilitate cross-chain data and liquidity transfers across multiple distributed-ledger networks. The project consists of two main

technological components: the deBridge messaging protocol, which enables the transmission of arbitrary data and instructions between supported blockchains, and the DeBridge Liquidity Network (DLN), an execution layer built to support asynchronous, non-custodial cross-chain trades without relying on traditional liquidity pools. The project is maintained by contributors to the deBridge ecosystem and is intended to provide developers and users with tools for interacting with decentralised systems in a multi-chain environment, subject to the availability, performance, and continued operation of the underlying technological infrastructure.

The DBR crypto-asset functions as an element within this broader technical framework. It is intended to interact with specific parts of the protocol's internal logic, such as governance parameters, validator-incentive mechanisms, staking modules, and fee-calculation structures, if and when these features are implemented or activated. Certain functionalities—such as staking, delegated slashing, or the use of DBR as a payment unit for validator services—remain contingent on technical implementation, future governance decisions, and operational priorities. There is no assurance that any proposed or potential functionalities will be introduced, remain active, or be accessible at all times.

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

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

<b>Name</b>	<b>Position</b>	<b>Business Address</b>
deBridge Foundation	Foundation entity responsible for DBR token operations, Reserve Fund, Treasury, grants, decentralization	Cayman Islands, KY – George Town Financial Center, Suite 303, 90 Fort Street, George Town, Grand Cayman, KY1-1104
DxTech Inc. (“deBridge”)	Panama entity operating core services, smart contracts, APIs	Panama, PA – Banking District, Advanced Tower, 1st Floor, Panama City
Alex Smirnov	CEO, Co-Founder, Project Lead	Could not be identified.
Yaroslav Artyukh	CTO, Co-Founder	Could not be identified.

### **D.6 Utility Token Classification**

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

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

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

## D.8 Plans for the token

This section provides an overview of the historical developments related to the DBR 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 DBR crypto-asset. Based on public information (sources: <https://debridge.com>, Foundation announcements, token launch disclosures; accessed 2025-12-08), several protocol upgrades, ecosystem initiatives, and token-related developments have been communicated that affect the evolution of the deBridge interoperability infrastructure and the role of the DBR token.

Past milestones:

- Initial Protocol Launch and Mainnet Activation (2021): In 2021, the deBridge interoperability system was introduced and deployed, marking the first production release of the cross-chain messaging and liquidity infrastructure that later became the foundation for the DBR token ecosystem. This initial launch established the technical architecture upon which subsequent protocol upgrades, validator operations, and governance structures were built.

- Season 1 Snapshot Completion (July 23, 2024):

The project finalized the Season 1 points snapshot, defining eligibility for the initial distribution of DBR.

- Public DBR Token Generation Event (TGE) (October 17, 2024): The DBR token was launched with an initial circulating supply of approximately 1.8 billion DBR (18% of total supply).

- Season 2 Launch and Distribution (2025): Season 2 of the points program continued accruing user activity. On November 19, 2025, the project executed the Season 2 claim event, distributing 300 million DBR (3% of total supply) to more than 770,000 eligible users.

- Reserve Fund Activation (June 2025): The deBridge Reserve Fund entered a pilot phase directing 100% of deBridge protocol earnings toward acquiring DBR via decentralized exchanges. As of July 24, 2025, accumulated holdings reached USD 28.65 million in a mix of DBR and major crypto-assets (USDC, SOL, ETH).

Future milestones:

- Progressive Transition to DAO Governance: The Foundation has stated that governance responsibilities will shift progressively from core contributors to the community. DBR token holders are expected to gain increasing authority over treasury decisions, protocol parameters, and ecosystem incentives.
- Validator Restaking and Slashing Module: Once deployed, staked DBR will be eligible for restaking to validators operating the deBridge messaging infrastructure. The module will enable slashable collateral to protect against validator downtime, censorship, or collusion, enhancing protocol security.

## D.9 Resource allocation

According to publicly available information found at <https://docs.debridge.foundation/faq-airdrop-season-1/dbr-tokenomics> (accessed on 2025-12-08), the DBR crypto-asset has a fixed total supply of 10,000,000,000 DBR. At the public Token Generation Event (TGE) on 17 October 2024, 1,800,000,000 DBR (18% of the total supply) entered circulation. This consisted of 1,000,000,000 DBR allocated to Community & Launch participants (10%), 300,000,000 DBR for the Ecosystem pool (3%), and 500,000,000 DBR assigned to the deBridge Foundation treasury (5%).

The remaining 82% of the total supply is subject to multi-year vesting schedules intended to align long-term incentives among ecosystem participants. The Community & Launch category receives a total of 2,000,000,000 DBR (20%), of which half was unlocked at TGE while the remainder vests quarterly over three years starting six months after TGE. The Ecosystem allocation comprises 2,600,000,000 DBR (26%), with 300,000,000 DBR available at TGE and the remaining 2,300,000,000 DBR vested quarterly over three years, likewise beginning six months after TGE.

Core Contributors are allocated 2,000,000,000 DBR in total (20%), with no tokens unlocked at TGE; 400,000,000 DBR unlock six months after TGE, and the remaining 1,600,000,000 DBR vest quarterly over three years. Strategic Partners receive 1,700,000,000 DBR (17%), with no TGE unlock; 340,000,000 DBR unlock after six months, followed by quarterly vesting of the remaining 1,360,000,000 DBR over three years. Validators are allocated 200,000,000 DBR (2%), with 40,000,000 DBR unlocking six months after TGE and quarterly vesting of the remaining 160,000,000 DBR for three years. The deBridge Foundation receives a total of 1,500,000,000 DBR (15%), of which 500,000,000 DBR were unlocked at TGE; the remaining 1,000,000,000 DBR vest quarterly over three years starting six months after TGE.

Certain community participants were subject to specific claim rules. The top 10% of Season 1 holders, representing roughly 76% of all Season 1 allocations, could claim 50% of their tokens at TGE, with the remainder available after six months, or alternatively claim 100% immediately with a 20% penalty. LFG vault participants could claim 50% at TGE, with the remaining 50% vesting for six months, while the remaining 90% of Season 1 users could claim their entire allocation at TGE.

Note: While wallet-level token balances can be verified on-chain, allocations to specific persons or entities cannot be independently confirmed, as public blockchain addresses cannot be reliably attributed to identifiable natural or legal persons. Consequently, the precise economic influence of

individual stakeholders cannot be determined. Token movements, changes in ownership, or internal re-allocations may occur without prior notice and could affect governance dynamics, market perceptions, or anticipated economic outcomes.

## **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**

The white paper concerns the admission to trading (i. e. ATTR).

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

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

### **E.3 Fundraising target**

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

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

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

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

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

### **E.6 Oversubscription acceptance**

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

### **E.7 Oversubscription allocation**

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

### **E.8 Issue price**

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

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

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

#### **E.10 Subscription fee**

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

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

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

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

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

#### **E.13 Targeted holders**

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

#### **E.14 Holder restrictions**

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

#### **E.15 Reimbursement notice**

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

#### **E.16 Refund mechanism**

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

#### **E.17 Refund timeline**

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

#### **E.18 Offer phases**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Crypto Risk Metrics GmbH has established, implemented, and documented comprehensive internal policies and procedures for the identification, prevention, management, and documentation of

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

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

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

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

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

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

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

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

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

According to public information available on the official website (<https://debridge.com>) and associated governance and documentation resources, the DBR token is a Solana-based SPL token intended to operate as the primary on-chain coordination mechanism within the deBridge ecosystem.

The DBR token is designed to facilitate decentralized decision-making within the deBridge protocol. Token holders may propose and vote on governance actions that determine configuration parameters of the protocol, such as validator whitelists, validator payout ratios, smart-contract upgrades, and treasury management decisions. Voting rights relate exclusively to technical and protocol-level features and do not extend to decisions regarding the operation, management, or assets of deBridge Foundation or affiliated entities. The full transition toward community-managed governance is planned to occur progressively as decentralization milestones are reached.

Within the deBridge network, DBR is used as a quantification unit for consumed computing resources. Validators maintaining the protocol's messaging and execution infrastructure may receive rewards denominated in DBR, and the token may be used as the medium for accounting validator incentives and redistributing network fees. These functionalities depend on the stable operation of the Solana network, the security of validator systems, the correct functioning of smart-contract modules, and the availability of governance-approved fee parameters.

The DBR 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 deBridge protocol environment. The actual usability of DBR depends on factors such as system stability, smart-contract execution, development progress, governance decisions, and the operational conditions of the Solana blockchain, which are outside the control of token holders.

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

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

- Staking for Governance: DBR holders are expected to be able to stake their tokens to participate in governance voting.

- Delegated Staking and Slashing Module: Once implemented, staked DBR may serve as collateral for messaging validators. Slashing conditions would apply in cases of validator misconduct (e.g., censorship, downtime, or collusion), thereby integrating DBR into the system's economic-security layer.

- Governance Functionality: Governance participation will continue to evolve as more responsibilities are transferred from the Foundation to the community.

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

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

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

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

#### **F.5 The type of submission**

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

#### **F.6 Crypto-asset characteristics**

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, and is available on the Solana network. The crypto-asset is fungible up to 6 digits after the decimal point. 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: "deBridge" according to the Digital Token Identifier Foundation ([www.dtif.org](http://www.dtif.org), DTI see F.13, FFG DTI see F.14 as of 2025-12-08).

### **F.8 Website of the issuer**

<https://debridge.foundation/>

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

2026-01-16

### **F.10 Publication date**

2026-01-25

### **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**

5BTQ61NXL

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

NT91TJWNC

### **F.15 Voluntary data flag**

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

### **F.16 Personal data flag**

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

### **F.17 LEI eligibility**

The issuer should be 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, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

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

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

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

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

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

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

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

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

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

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

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

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

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

Information on the future offers to the public of crypto-assets were not available at the time of writing this white paper (2025-12-08).

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

According to publicly available information available on the official website <https://debridge.com/> (accessed on 2025-12-08), the deBridge Foundation is allocated 1,500,000,000 DBR, representing 15% of the total DBR supply. Of this amount, 500,000,000 DBR were unlocked at the Token Generation Event on 17 October 2024, while the remaining 1,000,000,000 DBR are subject to a three-year quarterly vesting schedule beginning six months after TGE. These crypto-assets form part of the Foundation's treasury and are intended to support protocol development, ecosystem growth, liquidity initiatives, and other activities approved through governance processes. Note: While the allocation to the deBridge Foundation is publicly disclosed, on-chain wallet addresses associated with this allocation cannot be independently linked to specific natural persons. Token movements or internal treasury management actions may occur without prior notice and could affect the concentration of holdings and the future governance influence associated with these assets. The current token distribution can be traced on-chain: <https://solscan.io/token/DBRiDgJAMsM95moTzJs7M9LnkGErpbv9v6CUR1DXnUu5#holders>.

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

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

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

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

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

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

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

The admission to trading is sought.

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

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

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

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

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

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2025-12-03. However, it is possible to decrease the circulating supply by transferring crypto-assets to so-called "burn addresses". These are addresses from which the tokens are no longer intended to be transferred or accessed, effectively removing them from circulation.

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

For the crypto-asset in scope, the supply is limited to 10,000,000,000 units according to public information (Source: <https://debridge.foundation/> 2025-12-08). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The following applies to Solana:

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

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

Core functions of the Token Program:

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

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

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

`transfer()` → Transfers tokens between accounts

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

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

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

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

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

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

The following applies to Solana:

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

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

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

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

Security Protocols for Asset Custody and Transactions:

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

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

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

The crypto-asset in scope is implemented on the Solana network 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):

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

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

## 2. Proof of Stake (PoS):

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

selected to validate transactions and produce new blocks.

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

## Consensus Process

### 1. Transaction Validation:

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

### 2. PoH Sequence Generation:

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

cryptographic clock for the network.

### 3. Block Production:

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

### 4. Consensus and Finalization:

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

## Security and Economic Incentives

### 1. Incentives for Validators:

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

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

## 2. Security:

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

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

## 3. Economic Penalties:

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

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

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

The following applies to Solana:

### 1. Validators:

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

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

### 2. Delegators:

**Delegated Staking:** Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share the rewards earned by the validators. This is

intended to encourage widespread participation in securing the network and ensures decentralization.

### 3. Economic Security:

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

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

### Fees Applicable on the Solana Blockchain

#### 1. Transaction Fees:

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

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

#### 2. Rent Fees:

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

#### 3. Smart Contract Fees:

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

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

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

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

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

## H.8 Audit

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

## H.9 Audit outcome

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

# Part I – Information on risks

## I.1 Offer-related risks

### 1. Regulatory and Compliance

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

### 2. Trading venue and connection risk

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

### 3. Market formation and liquidity conditions

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

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

#### 4. Counterparty and service-provider dependence

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

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

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

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

#### 5. Operational and information risks

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

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

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

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

### 1. Insolvency of the issuer

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

### 2. Legal and regulatory risks

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

### 3. Operational risks

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

### 4. Governance and decision-making

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

### 5. Reputational risks

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

### 6. Counterparty dependence

The issuer may depend on third-party providers for certain core functions, such as technology development, marketing, legal advice, or infrastructure. If these partners discontinue their services, change ownership, or underperform, the issuer's ability to operate the project or maintain investor

communication may be impaired. This could disrupt project continuity or undermine market confidence, ultimately affecting the crypto-asset's value.

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

#### 1. Valuation risk

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

#### 2. Market volatility risk

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

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

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

#### 4. Asset security risk

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

#### 5. Fraud and scam risk

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

#### 6. Legal and regulatory reclassification risk

Legislative or regulatory changes in the European Union or in the Member State where the crypto-asset is admitted to trading may alter its legal classification, permitted uses, or tradability. In third

countries, the crypto-asset may be treated as a financial instrument or security, which can restrict its offering, trading, or custody.

#### 7. Absence of investor protection

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

#### 8. Counterparty risk

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

#### 9. Reputational risk

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

#### 10. Community and sentiment risk

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

#### 11. Macroeconomic and interest-rate risk

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

#### 12. Taxation risk

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

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

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

#### 14. Market-abuse risk

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

#### 15. Legal ownership and jurisdictional risk

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

#### 16. Concentration risk

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

### **I.4 Project implementation-related risks**

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

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

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

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

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

### **I.5 Technology-related risks**

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

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

### 1. Blockchain dependency risk

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

### 2. Smart contract vulnerability risk

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

### 3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

### 4. Network security risks

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

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

### 5. Bridge and interoperability risk

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

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

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

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

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

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

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

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

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

#### 10. Decentralisation claim risk

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

### **I.6 Mitigation measures**

None.

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

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

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

Crypto Risk Metrics GmbH

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

39120077M9TG001FE242

#### **S.3 Name of the cryptoasset**

deBridge

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

The crypto-asset in scope is implemented on the Solana network 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):

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

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

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

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

selected to validate transactions and produce new blocks.

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

## Consensus Process

### 1. Transaction Validation:

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

### 2. PoH Sequence Generation:

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

cryptographic clock for the network.

### 3. Block Production:

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

### 4. Consensus and Finalization:

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

## Security and Economic Incentives

### 1. Incentives for Validators:

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

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

### 2. Security:

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

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

### 3. Economic Penalties:

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

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

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

The following applies to Solana:

### 1. Validators:

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

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

### 2. Delegators:

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

### 3. Economic Security:

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

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

## Fees Applicable on the Solana Blockchain

### 1. Transaction Fees:

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

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

### 2. Rent Fees:

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

### 3. Smart Contract Fees:

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

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

2024-11-19

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

2025-11-19

## **S.8 Energy consumption**

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

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

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

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

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

### **S.11 Energy intensity**

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

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

### **S.14 GHG intensity**

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

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

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

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

