CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG PPDH6B273

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified at 2025-12-12.

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 Dash (DASH) referred to in this white paper is a crypto-asset other than EMTs or ARTs, which is native to the Dash blockchain and issued on the Tron

blockchain as of 2025-12-08, and according to the DTI FFG shown in F.14. The maximum supply of the crypto-asset is 18,900,000 units. The first on-chain activity of the crypto-asset originates from the Dash genesis block (hash: 00000ffd590b1485b3caadc19b22e6379c733355108f107a430458cdf3407ab6, dated 2014-01-19, source: https://explorer.dash.org/insight/block/00000ffd590b1485b3caadc19b22e6379c733355108f107a430458cdf3407ab6, accessed 2025-12-08). The first on-chain activity on the Tron network is recorded under transaction hash 3317f011b37c2041582535858d405cf2e944156289c9417447cde08f5aa6c67f, dated 2019-07-08 (source: https://tronscan.org/#/transaction/3317f011b37c2041582535858d405cf2e944156289c9417447cde08f5aa6c67f, accessed 2025-12-08).

The Dash crypto-asset (DASH) is the native currency of the Dash blockchain and forms the basis of a payments-focused network designed to enable fast, low-cost, and secure digital transactions. The network operates through a two-tier architecture combining Proof-of-Work mining with an incentivized masternode layer that provides additional services such as near-instant transaction locking, optional transaction-level privacy, and decentralized governance. DASH is used to pay transaction fees on the network, and certain network functions - including operating masternodes and participating in governance - require holders to commit DASH as collateral. DASH does not grant holders any ownership, profit participation, or governance rights over any legal entity; all functionalities arise solely from the operation of the protocol.

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

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

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is "a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer". This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or 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 repective 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 39120077M9TG0O1FE242.

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

established progressively and can be realistically considered fully operational since approximately 2024.

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

2024 (unaudited): negative EUR 50.891,81

2023 (unaudited): negative EUR 27.665,32

2022: EUR 104.283,00.

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

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

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

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

With the regulatory environment now taking shape and the platform commercially validated, it is assumed that the effects of the strategic developments will continue to

materialize in 2026. The company foresees further scalability of its technology and growing market demand for regulatory compliance tools in the European crypto-asset sector.

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

According to public information, the Dash network was launched on 2014-01-18 by Evan Duffield, who developed the original Dash protocol and authored its initial technical components, including the X11 chained-hash algorithm and the Dark Gravity Wave (DGW) difficulty-adjustment mechanism.

While Evan Duffield initiated the project, the Dash blockchain has, since its launch, been maintained by a global network of independent participants such as miners, masternodes, developers, and users, rather than by a formal legal entity.

At the time of writing this white paper (2025-12-08), the issuer of the crypto-asset remains unknown in the sense required under applicable legislation, as no legally constituted issuing entity exists.

B.3 Legal form

The crypto-asset does not appear to be issued by a formal company or foundation in the traditional sense. Instead, it follows a decentralized, community-driven approach exercised within the Dash protocol.

B.4. Registered address

Not applicable.

B.5 Head office

Not applicable.

B.6 Registration date

Not applicable.

B.7 Legal entity identifier

Not applicable.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Not applicable.

B.11 Business activity

Not applicable.

B.12 Parent company business activity

Not applicable.

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

C.1 Name

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

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-Asset white paper Preparation

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

C.10 Members of the Management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

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

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

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

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

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

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Dash", Short Name: "DASH" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-12-08).

D.2 Crypto-assets name

Long Name: "Dash" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-12-08).

D.3 Abbreviation

Short Name: "DASH" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-12-08).

D.4 Crypto-asset project description

According to public information, including the Dash whitepaper, the official Dash.org website, and related technical documentation (accessed on 2025-12-08), the crypto-asset project associated with DASH concerns the development and operation of a distributed, two-tier blockchain network originally founded by Evan Duffield. The project follows architectural principles comparable to early cryptocurrencies such as Bitcoin, combining a Proof-of-Work–based mining layer with a second layer of collateralised service nodes ("masternodes"). The network is designed to facilitate peer-to-peer digital payments, rapid transaction settlement, and additional network services, subject to the availability and continued functioning of the underlying software infrastructure.

The first tier of the system consists of miners who validate and order transactions using the X11 hashing algorithm together with the Dark Gravity Wave difficulty-adjustment mechanism. These components define block creation, emission parameters, and network security. The second tier consists of masternodes, which perform specialised services such as InstantSend transaction locking, CoinJoin-based privacy functions, decentralised governance voting, treasury-budget processing, and enhanced chain-security mechanisms such as ChainLocks. Masternode operators must prove control over the required collateral and maintain required service levels, forming part of the protocol's Proof-of-Service framework.

Within this architecture, the DASH crypto-asset functions as a native digital unit recorded on the Dash blockchain. It is used to pay transaction fees, to serve as collateral for operating masternodes and evonodes, and to participate in protocol-level governance processes where network participants make decisions on matters such as budget allocations. These roles are technical in nature and depend entirely on protocol design, network conditions, and the operational continuity of the distributed system. The DASH crypto-asset does not represent ownership, profit participation, governance rights in a legal sense, or any other legally enforceable claims against an issuer or related entity.

As with other open and decentralised blockchain networks, the ongoing development, scope of available features, and long-term sustainability of the Dash project depend on

independent contributors, system incentives, node participation, market dynamics, and software maintenance. Any future enhancements or feature changes are subject to community processes and may evolve over time. No assurance can be given that specific functionalities will be introduced, continue to exist, or remain accessible under all circumstances.

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

Name	Position	Business Address
Evan Duffield	Founder of Dash (not active)	Could not be identified.
Dash Core Group, Inc.	Funded contractor responsible for core development, documentation, ecosystem support, and management of key services within the Dash Network	US-108 Lakeland Ave, Dover, Kent County, Delaware 19901, United States
Samuel Westrich	CTO, Dash Core Group, Inc.	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 Dash 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, and future changes may have adverse effects for token holders. Based on publicly available information (sources: https://www.dash.org, https://docs.dash.org, accessed 2025-12-08), several protocol-level and project-level milestones have shaped the development of the Dash network and the role of its native crypto-asset.

Past milestones:

- Launch and Early Network Features (2014):

The Dash blockchain launched with the X11 hashing algorithm, the Dark Gravity Wave (DGW) difficulty adjustment, and the original Masternode system. PrivateSend (formerly Darksend) was introduced as an optional privacy-enhancing feature.

- Governance System and InstantSend (2015):

Dash rebased to Bitcoin Core and released InstantSend (originally InstantX), enabling instant transaction locking. The protocol's on-chain governance system was introduced, culminating in the first treasury-funded superblock on 7 September 2015, establishing Dash as one of the earliest decentralized autonomous organizations.

- Scaling Vote (2016):

Masternode operators approved a consensus change to increase block size to 2 MB to ensure future capacity growth.

Dash Platform MVP Testnet – Evonet (Q4 2019):

Launch of the first public testnet for Dash Platform, including early versions of DAPI, identities, documents, and the Dash Platform Name Service (DPNS).

- Governance Accessibility Improvements (2022 – Core v0.18):

The governance proposal fee was lowered from 5 DASH to 1 DASH following a network-approved change, reducing barriers to community participation.

- Treasury Expansion and Core Improvements (2023 – v20):

The DAO approved an increase in the treasury budget from 10% to 20% of block rewards. Sentinel, formerly a required external daemon, was deprecated and integrated into Dash Core.

- Platform Activation (2024 – v21 & Evolution Platform Chain):

The Masternode Reward Reallocation hard fork activated in July 2024, enabling Dash Platform chain launch. By September 2024, Platform was activated on mainnet, introducing DPNS usernames and DashPay smart-contract components.

Future milestones:

- DashPay iOS Wallet (target: Q4 2025):

Release of the DashPay wallet for iOS, enabling creation of contested and non-contested usernames, username-based payments, and governance-integrated features for masternode owners.

- Dash Platform v3.0 (target: 2026):

Integration of a smart-contracts virtual machine to enable more expressive on-chain computation within the Platform layer.

- Dash Platform v4.0 (target: 2026):

Implementation of the Inter-Blockchain Communication (IBC) protocol, enabling permissionless cross-chain data and asset relaying.

All described future developments represent intended or potential milestones only. They remain dependent on technological feasibility, resource allocation, regulatory considerations, and general project priorities. There is no certainty that these developments will occur, occur as described, or be maintained in the long term. Deviations from the roadmap may occur without prior notice, and changes may negatively affect the usability or relevance of the token.

D.9 Resource allocation

According to public information found at https://www.dash.org/roadmap/ (accessed on 2025-12-08), no initial allocation of financial or crypto-asset resources was made toward the creation or launch of the Dash project. The crypto-asset emission began exclusively with the genesis block mined on 18 January 2014, and all units of DASH have been created through the ongoing Proof-of-Work mining process.

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 18,900,000 units. As of December 8, 2025, approximately 12,510,688 units are in circulation.

However, the number of units actively available on the market may differ from the circulating supply reported by public sources. A portion of the already-mined units may be held in long-term or dormant wallets, may be considered unrecoverable due to lost private keys, or may be concentrated among holders who do not regularly transact. These factors effectively reduce the amount of crypto-assets that can be traded at any given time.

Consequently, while the maximum supply provides a clear upper limit, the effective market float is influenced by wallet activity, long-term holding patterns, and the share of units that are permanently inaccessible. These dynamics can affect liquidity and may contribute to price volatility over time.

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 Dash documentation website (source: https://docs.dash.org/en/stable/, accessed 2025-12-08) and supporting technical resources, DASH is the native crypto-asset of the Dash blockchain. It operates within a two-tier decentralized network architecture designed to support peer-to-peer payments, transaction validation, and governance-related coordination across the protocol. As a native crypto-asset, DASH exists directly on the Dash ledger and is created through mining activities performed under the network's consensus rules.

Technical and Protocol-Level Roles of DASH:

On-chain payments and fee settlement: DASH functions as the medium used to pay transaction fees required for the processing and confirmation of transactions on the Dash blockchain. These fees compensate the validator sets operating both layers of the network. Payment transactions on Dash can be executed instantly using protocol features such as InstantSend, which rely on masternode quorums to lock transactions before final settlement. Fee levels depend on data size and network conditions.

Coordination unit for validator incentives: DASH serves as the crypto-asset used to account for and distribute block-subsidy rewards to both miners (first-tier Proof of Work validators) and masternodes or evonodes (second-tier Proof of Service validators). Newly minted DASH from each block is programmatically split between:

- miners (20% of the block subsidy),

- masternodes/evonodes (60% of the block subsidy), and

- the decentralized governance budget (20% of the block subsidy).

This use of DASH as a unit of account for protocol incentives supports the continued operation of both tiers of the network and the provision of services such as InstantSend and CoinJoin.

Collateral for operating a masternode or evonode: Running a masternode requires 1,000 DASH as collateral, and running an evonode (supporting Dash Platform services) requires 4,000 DASH. This collateral must remain continuously under the control of the operator. If it is moved, the node becomes ineligible for participation and reward selection. DASH therefore functions as the technical bonding asset that enables operators to provide second-tier validation, transaction-locking services, and, for evonodes, platform-related functions.

Governance-Related Coordination Uses: Participation in proposal submission and network funding decisions

Submission of a governance proposal to the Dash network requires a fee of 1 DASH, which is burned. This mechanism is designed to prevent spam and ensure that the decentralized treasury is used for meaningful contributions to the network. Voting power is exercised by masternode operators, each controlling one vote per masternode. All governance decisions relate exclusively to protocol-level funding allocations and maintenance of open-source development and do not extend to ownership or control rights over any legal entity.

The DASH 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 Dash protocol environment. The actual usability of DASH depends on factors such as system stability, code execution, development progress, governance decisions, and the operational conditions of the Dash 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:

Future milestones:

- DashPay iOS Wallet (target: Q4 2025):

Release of the DashPay wallet for iOS, enabling creation of contested and non-contested usernames, username-based payments, and governance-integrated features for masternode owners.

- Dash Platform v3.0 (target: 2026):

Integration of a smart-contracts virtual machine to enable more expressive on-chain computation within the Platform layer.

- Dash Platform v4.0 (target: 2026):

Implementation of the Inter-Blockchain Communication (IBC) protocol, enabling permissionless cross-chain data and asset relaying.

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 both as the native crypto-asset of the Dash blockchain and as a representation on the Tron network. On the Dash network, the crypto-asset is fungible up to 8 digits after the decimal point, with one DASH corresponding to 100,000,000 duffs. On the Tron 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 crypto-asset are limited to potential technical features within the relevant platform environments. 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: "Dash" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-12-08).

F.8 Website of the issuer

No formal issuer can be identified for the Token. Further information regarding the protocol, the broader ecosystem, and the Token is available at: https://www.dash.org/.

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

The intended admission to trading is 2026-01-15.

F.10 Publication date

The intended publication date is 2026-01-15.

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, where available

M5D76SHV5, J7WG2WKPP

F.14 Functionally fungible group digital token identifier, where available

PPDH6B273

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

Not applicable.

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

As the issuer could not be determined, no information about retained assets by the issuer itself were available at the time of drafting this white paper (2025-12-08).

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 2025-12-08.

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 18,900,000 units according to public information (Source: https://docs.dash.org, accessed 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 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 native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

The following applies to Dash:

The crypto-asset operates according to a defined set of protocols and technical standards designed to support its two-tier architecture, network security, transaction processing, and upgrade governance. The project builds on the original Bitcoin design but extends it through a Masternode layer, privacy mechanisms, and quorum-based instant transaction confirmation. Key standards are summarized below.

1. Network Protocols

– The network uses a two-tier architecture consisting of traditional Proof of Work (PoW) miners and a second layer of incentivized full nodes known as Masternodes, as originally introduced in the Dash whitepaper.

– PoW mining uses the X11 chained hashing algorithm, which sequentially combines eleven SHA-3 candidate hashes.

– Masternodes operate under a Proof of Service (PoSe) requirement, ensuring they remain online, synchronized, and responsive to the network.

– Masternode consensus functions rely on deterministic ordering, pseudo-random selection, and trustless quorums to execute sensitive tasks such as InstantX/InstantSend locking and privacy operations.

– The P2P layer uses message types such as Masternode Announce and Masternode Ping to propagate the active Masternode set and maintain liveness.

– Quorums of selected Masternodes verify service quality and enforce PoSe requirements. Approximately 1% of the network is checked each block, ensuring high service reliability.

– InstantX/InstantSend uses Masternode quorums to lock transaction inputs, resulting in near-instant irreversible settlement.

– ChainLocks (specified later in DIP-0008) extend this approach by allowing quorums to finalize blocks immediately upon mining.

2. Transaction and Address Standards

– Dash uses a UTXO-based transaction model derived from Bitcoin, with enhancements for privacy mixing, multi-party transaction construction, and deterministic Masternode metadata.

– Standard address formats include Pay-to-PubKey-Hash (P2PKH) and Pay-to-Script-Hash (P2SH), with Base58Check encoding.

– Transactions follow the standard input/output script model (scriptSig and scriptPubKey), using ECDSA over secp256k1 for signature generation.

– Special Transactions defined in DIP-0002 introduce structured fields for Masternode registration, updates, and other non-financial metadata required for deterministic network behavior.

– Darksend (now CoinJoin) provides decentralized privacy using denominations (0.1, 1, 10, 100 DASH) and multi-session chaining, as described in detail in the original whitepaper.

– Fees are proportional to transaction size and paid from the block subsidy. Block rewards are split deterministically between miners, Masternodes, and the governance treasury.

– InstantSend transactions rely on quorum-validated input locks rather than block confirmations, enabling secure real-time settlement.

3. Blockchain Data Structure & Block Standards

– The blockchain uses an 80-byte header format inherited from Bitcoin containing the previous block hash, Merkle root, timestamp, difficulty target, and nonce.

– Blocks are mined approximately every 2.6 minutes, with difficulty adjusted every block using the Dark Gravity Wave (DGW) algorithm to stabilize issuance even under volatile hash rates.

– All blocks must include a coinbase transaction, whose outputs cannot be spent for 100 blocks.

– Transactions inside each block are organized in a Merkle Tree, enabling lightweight clients to verify proofs using Simplified Payment Verification (SPV).

– Block reward distribution follows a fixed formula: a portion to miners, a larger portion to Masternodes, and 20% reserved for monthly governance superblocks.

– The Masternode payment system enforces correctness by rejecting blocks that fail to pay the designated Masternode determined through deterministic selection.

– The whitepaper's mining supply chart illustrates a long-term issuance schedule where rewards decline by approximately 7% per year rather than halving events, extending issuance to around the year 2150.

4. Upgrade & Improvement Standards

Dash uses the Dash Improvement Proposal (DIP) framework to specify new features and consensus changes. Three representative finalized or widely implemented DIPs are listed below.

– DIP-0003 (Deterministic Masternode Lists)

Defines on-chain deterministic lists that ensure all nodes arrive at the same Masternode view. This eliminates inconsistencies in quorum formation and is foundational for evolved Masternode features.

– DIP-0008 (ChainLocks)

Introduces LLMQ-based block signing that provides near-instant finality by locking blocks as soon as they are mined. ChainLocks prevent reorganization attacks and significantly increase chain security.

– DIP-0023 (Enhanced Hard Fork Mechanism)

Specifies a structured activation method for consensus changes, improving the reliability and predictability of network upgrades. This replaces reliance on legacy mechanisms such as Sporks for certain categories of changes.

The following applies to Tron:

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

1. Network Protocols

The crypto-asset operates on the TRON blockchain, which is based on a decentralized, peer-to-peer networking architecture. Nodes communicate using a combination of gRPC

and HTTP interfaces, with gRPC serving as the primary high-performance channel for block, transaction, and contract-execution communication.

– TRON maintains several network environments: the Mainnet (production network for transactions with economic value), test networks such as Shasta and Nile for development, and private networks that can be deployed locally for isolated testing scenarios.

– Node participation is open to all: Fullnodes store and validate the complete blockchain history and expose APIs for querying and broadcasting transactions; Lite Fullnodes synchronize from a reduced snapshot and support fast startup for general applications requiring only recent state.

– The P2P layer supports message propagation, block relay, and node discovery, including support for optimizations such as compressed P2P messages and DNS-based node discovery as introduced in later TRON Improvement Proposals (TIPs).

– The network is designed around Delegated Proof of Stake (DPoS), where Super Representatives (SRs) maintain block production and consensus by collaboratively verifying and broadcasting blocks.

2. Transaction and Address Standards

TRON uses an account-based model in which each account is controlled by an asymmetric key pair.

– Addresses exist in two representations: a Hex format starting with the prefix 41, and a Base58Check-encoded representation beginning with T. Both refer to the same underlying account.

– All state-changing operations are formulated as signed transactions, which include the contract payload (raw_data.contract), timestamp, expiration, and a reference block indicator (TAPOS) to prevent replay on historical forks.

– Core system contract types define basic functionality at the protocol level, including TransferContract for TRX transfers, TransferAssetContract for TRC-10 transfers, FreezeBalanceV2Contract and UnfreezeBalanceV2Contract for staking under Stake 2.0, and TriggerSmartContract for invocations of smart-contract logic.

– Smart contracts run on the TRON Virtual Machine (TVM), and execution requires the caller to specify a fee_limit parameter, which caps the maximum Energy consumption of the transaction.

– Token and asset standards include TRC-10 (protocol-level assets not requiring smart contracts), TRC-20 (fungible smart-contract assets analogous to ERC-20), TRC-721 (non-fungible crypto-asset standard), and TRC-1155 (multi-asset standard allowing fungible and non-fungible items within a single contract). These standards are defined through the TRON Improvement Proposal (TIP) process and form part of the broader interoperability specification of the TRON ecosystem.

3. Blockchain Data Structure and Block Standards

The blockchain consists of sequentially chained blocks, each containing a block header and a list of validated transactions.

– Consensus follows a Delegated Proof of Stake model where 27 elected Super Representatives produce blocks in three-second intervals. Within each time slot, the designated SR aggregates transactions, verifies them, constructs a block, signs it, and broadcasts it to the network.

– A block is considered irreversible once more than 70% of SRs (at least 19 of 27) approve it, at which point the block becomes solidified in the canonical history.

– Each block header records metadata such as the block number, parent block hash, Merkle root of the transaction trie, timestamp, and the address and signature of the producing SR.

– TRON enforces a maximum block size of approximately 2,000,000 bytes, enabling high-frequency block production while keeping propagation delays predictable.

– The blockchain state includes account balances, smart-contract storage, resource allocations (Bandwidth and Energy), and system parameters, all maintained by the TVM state model and updated deterministically during transaction execution.

4. Upgrade and Improvement Standards

Protocol upgrades on TRON follow the TRON Improvement Proposal (TIP) framework, which defines standards for consensus rules, networking, APIs, token formats, and TVM behavior.

– Super Representatives (SRs) govern adjustable protocol parameters through an on-chain proposal system. Proposals remain open for three days and are approved when at least 18 of the 27 SRs vote in favor, after which the updated parameters are implemented via client releases.

– TIPs specify changes such as resource-model adjustments, Energy-cost updates, new TVM instructions, or EVM-compatibility features, enabling iterative development without requiring frequent hard forks.

– Smart-contract upgradeability is achieved at the application layer through patterns such as proxy-based architectures, which separate contract storage from logic and allow implementation contracts to be replaced without modifying stored data.

H.3 Technology used

The crypto-asset in scope is native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

The following applies to Dash:

1. Private Key Management

Dash relies on private-key management practices derived from Bitcoin. Users must securely store their private keys and recovery phrases to retain control over their crypto-assets. Private/public key pairs are generated through the Elliptic Curve Digital

Signature Algorithm (ECDSA) using the secp256k1 curve, as described in the Dash protocol. Dash Core uses hierarchical deterministic (HD) key generation, enabling wallets to derive multiple keys from a single seed phrase. For masternodes, separate keys exist for collateral control, voting, and operation, preventing operational delegation from affecting control of funds.

2. Cryptographic Integrity

Dash employs multiple cryptographic components to validate transactions and maintain ledger integrity. Transaction authorization uses ECDSA signatures with the secp256k1 curve, while transaction identifiers and block linking rely on double SHA-256 hashing. For Proof of Work, Dash applies the X11 hashing algorithm, a chained sequence of eleven hash functions designed to enhance computational security and reduce predictability compared to single-algorithm designs. These mechanisms collectively underpin the secure creation, validation, and propagation of transactions across the network.

The following applies to Tron:

1. Private Key Management

TRON accounts are controlled through ECDSA key pairs (secp256k1). The private key is required for authorizing all transactions and must be protected securely, as anyone with access can control the corresponding account. Users typically secure their keys through hardware wallets or other cold-storage methods. TRON also supports advanced permission management, allowing accounts to assign multiple keys with weighted signatures across Owner, Active, and Witness permission groups.

2. Decentralized Ledger

The TRON blockchain maintains a decentralized ledger of all transfers and contract interactions, intended to provide a verifiable and tamper-resistant transaction history. Blocks contain the Merkle root of included transactions and references to prior blocks, preserving data integrity through hash chaining.

3. Cryptographic Integrity and Hashing

TRON uses Keccak-256 for address generation and transaction hashing. Signatures rely on ECDSA to authenticate the sender and prevent unauthorized modification of transaction data. Verification reconstructs the signer's public key from the signature to confirm that it matches the originating account. Hashing also supports Merkle trie state management in block headers. The TVM provides precompiled cryptographic functions and implements distinct internal hashing behavior for certain operations.

4. TRC Standards for Fungible and Non-Fungible Assets

TRON supports multiple token standards.

– TRC-10: A protocol-level fungible asset standard issued via system contracts, requiring a 1,024 TRX creation fee and allowing only one issuance per account. Transfers use the TransferAssetContract.

– TRC-20: A fungible smart-contract standard compatible with ERC-20, defining functions for supply, balance queries, transfers, and allowances, along with Transfer and Approval events.

– TRC-721: A non-fungible token standard compatible with ERC-721, requiring implementation of TRC-721 and TRC-165 interfaces.

H.4 Consensus mechanism

The crypto-asset in scope is native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

The following applies to Dash:

The Dash blockchain relies on a two-tier hybrid consensus mechanism combining Proof-of-Work (PoW) and Proof-of-Service (PoSe). In the first tier, miners perform PoW using the X11 chained hashing algorithm to propose new blocks. Miners repeatedly compute the hash of the block header and a nonce until the output meets the network's difficulty target. This process is computationally hard but easy for nodes to verify. Once a valid

block is found, it is broadcast to the network and, if accepted, added to the chain. Difficulty adjusts every block through the Dark Gravity Wave algorithm to maintain an intended average block time of roughly 2.6 minutes. These characteristics are described in the Dash technical documentation and the original whitepaper, which outlines the X11 algorithm and DGW difficulty adjustment model.

The second tier consists of Masternodes, which operate under PoSe. Masternodes are collateral-backed full nodes that must remain online and responsive. They verify that blocks comply with network rules and can reject invalid blocks, adding an enforcement layer on top of PoW. Masternode quorums also provide fast finality through ChainLocks: once a quorum signs a block, competing blocks at that height are rejected, making chain reorganizations substantially more difficult. InstantSend uses similar quorums to lock transaction inputs within seconds, preventing double spending before block confirmation. The network follows the longest valid chain but prioritizes ChainLocked blocks, making past alterations computationally and economically impractical.

The following applies to Tron:

TRON uses a Delegated Proof-of-Stake (DPoS) consensus mechanism in which holders of the native crypto-asset stake their units to obtain voting rights. These votes determine the 27 Super Representatives (SRs) that take turns proposing and validating blocks. A new block is produced approximately every three seconds, following the slot schedule assigned at the beginning of each six-hour epoch. If an SR misses its slot, the network moves to the next validator without delay.

Blocks become irreversible once more than 70% of SRs (at least 19 of 27) build subsequent blocks on top of them, providing economic finality. Governance and parameter changes are implemented through an on-chain proposal system, with only

SRs eligible to vote. DPoS is intended to provide rapid block production, low energy consumption, and predictable finality through an elected validator set.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

The following applies to Dash:

The crypto-asset's incentive mechanism is structured to reward participants for securing both layers of the network. Dash operates a two-tier architecture: miners secure the blockchain through Proof of Work (PoW), while masternodes and evonodes secure the service layer through Proof of Service (PoSe). Both groups receive a share of the block subsidy and transaction fees.

Incentives for Miners (Tier 1 – PoW)

Miners validate transactions and add new blocks by performing PoW using the X11 hashing algorithm. For each valid block, miners receive a portion of the newly generated block subsidy as well as a share of the transaction fees included in the block. Following the updated reward allocation model, miners receive 20% of the total block subsidy and 25% of the transaction fees. These incentives promote accurate validation and help maintain the security of the decentralized ledger.

Incentives for Masternodes and Evonodes (Tier 2 – PoSe)

Masternodes and evonodes support network services such as InstantSend, CoinJoin, and ChainLocks, providing transaction locking, mixing, and governance functions. To compensate operators for this service commitment and collateral requirement (1,000 DASH per masternode), they collectively receive 60% of the block subsidy. This amount is further split between masternodes on the Core chain and the Platform credit pool

that compensates evonodes. They also receive 75% of the transaction fees. Nodes failing to meet PoSe requirements are removed from the payment rotation, ensuring that rewards flow only to nodes providing reliable service.

Transaction Fees and Fee Dynamics

Transaction fees are paid by the user who creates the transaction. Fees are based on the size of the signed transaction (in bytes) and remain predictable and generally low. A commonly used standard fee is 0.00001 DASH per kB. Transactions offering higher fees per byte may be prioritized by miners when block space is limited. While typical fees remain stable, they may increase during periods of elevated demand. CoinJoin transactions are usually free, aside from an occasional small fee applied randomly to mitigate spam.

The following applies to Tron:

Super Representatives earn 8 units of the native crypto-asset for each block they produce, while an additional 128 units per block are shared among all SRs and SR partners based on votes received. Voters obtain rewards through staking and voting, with SRs deducting a commission before distributing payouts. This incentive structure is intended to maintain active participation and reliable block production.

Transactions and smart-contract executions consume Bandwidth and Energy. Users can obtain these resources by staking or, if insufficient, by burning the native crypto-asset at fixed rates. Certain protocol actions such as becoming an SR candidate, issuing assets, creating accounts, or updating permissions carry dedicated execution fees, and optional costs apply for multi-signature transactions or memos.

While the protocol does not use slashing, resource-based penalties apply. Failed contract executions may result in increased Energy deductions, and the dynamic Energy model raises future costs for contracts that heavily consume network resources. These measures are intended to preserve system stability and prevent resource abuse.

H.6 Use of distributed ledger technology

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

H.7 DLT functionality description

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

H.8 Audit

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

Regulatory frameworks applicable to crypto-asset services in the European Union and in third countries are evolving. Supervisory authorities may introduce, interpret, or enforce

rules that affect (i) the eligibility of this crypto-asset for admission to trading, (ii) the conditions under which a crypto-asset service provider may offer trading, custody, or transfer services for it, or (iii) the persons or jurisdictions to which such services may be provided. As a result, the crypto-asset service provider admitting this crypto-asset to trading may be required to suspend, restrict, or terminate trading or withdrawals for regulatory reasons, even if the crypto-asset itself continues to function on its underlying network.

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

Volatility: The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the

crypto-asset at or close to a previously observed price, even though no negative project-specific event has occurred.

4. Counterparty and service-provider dependence

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

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

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

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

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

Network upgrades or disagreements among node operators or validators can result in blockchain “forks”, where the blockchain splits into two or more incompatible versions that continue separately from a shared past. This may lead to duplicate token representations or incompatibilities between exchanges and wallets. Until consensus

stabilises, trading or transfers may be disrupted or misaligned. Such situations may be difficult for retail holders to navigate, particularly when trading platforms or wallets display inconsistent token information.

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the cryptoasset

Dash

S.4 Consensus Mechanism

The crypto-asset in scope is native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

The following applies to Dash:

The Dash blockchain relies on a two-tier hybrid consensus mechanism combining Proof-of-Work (PoW) and Proof-of-Service (PoSe). In the first tier, miners perform PoW using the X11 chained hashing algorithm to propose new blocks. Miners repeatedly compute the hash of the block header and a nonce until the output meets the network's difficulty target. This process is computationally hard but easy for nodes to verify. Once a valid block is found, it is broadcast to the network and, if accepted, added to the chain. Difficulty adjusts every block through the Dark Gravity Wave algorithm to maintain an intended average block time of roughly 2.6 minutes. These characteristics are described in the Dash technical documentation and the original whitepaper, which outlines the X11 algorithm and DGW difficulty adjustment model.

The second tier consists of Masternodes, which operate under PoSe. Masternodes are collateral-backed full nodes that must remain online and responsive. They verify that blocks comply with network rules and can reject invalid blocks, adding an enforcement layer on top of PoW. Masternode quorums also provide fast finality through ChainLocks: once a quorum signs a block, competing blocks at that height are rejected, making chain reorganizations substantially more difficult. InstantSend uses similar quorums to lock transaction inputs within seconds, preventing double spending before block confirmation. The network follows the longest valid chain but prioritizes ChainLocked blocks, making past alterations computationally and economically impractical.

The following applies to Tron:

TRON uses a Delegated Proof-of-Stake (DPoS) consensus mechanism in which holders of the native crypto-asset stake their units to obtain voting rights. These votes determine the 27 Super Representatives (SRs) that take turns proposing and validating blocks. A new block is produced approximately every three seconds, following the slot schedule assigned at the beginning of each six-hour epoch. If an SR misses its slot, the network moves to the next validator without delay.

Blocks become irreversible once more than 70% of SRs (at least 19 of 27) build subsequent blocks on top of them, providing economic finality. Governance and parameter changes are implemented through an on-chain proposal system, with only SRs eligible to vote. DPoS is intended to provide rapid block production, low energy consumption, and predictable finality through an elected validator set.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is native to the Dash blockchain network and is also issued on the Tron blockchain, following the standards described below.

The following applies to Dash:

The crypto-asset's incentive mechanism is structured to reward participants for securing both layers of the network. Dash operates a two-tier architecture: miners secure the blockchain through Proof of Work (PoW), while masternodes and evonodes secure the service layer through Proof of Service (PoSe). Both groups receive a share of the block subsidy and transaction fees.

Incentives for Miners (Tier 1 – PoW)

Miners validate transactions and add new blocks by performing PoW using the X11 hashing algorithm. For each valid block, miners receive a portion of the newly generated block subsidy as well as a share of the transaction fees included in the block. Following the updated reward allocation model, miners receive 20% of the total block subsidy and 25% of the transaction fees. These incentives promote accurate validation and help maintain the security of the decentralized ledger.

Incentives for Masternodes and Evonodes (Tier 2 – PoSe)

Masternodes and evonodes support network services such as InstantSend, CoinJoin, and ChainLocks, providing transaction locking, mixing, and governance functions. To compensate operators for this service commitment and collateral requirement (1,000 DASH per masternode), they collectively receive 60% of the block subsidy. This amount is further split between masternodes on the Core chain and the Platform credit pool that compensates evonodes. They also receive 75% of the transaction fees. Nodes failing to meet PoSe requirements are removed from the payment rotation, ensuring that rewards flow only to nodes providing reliable service.

Transaction Fees and Fee Dynamics

Transaction fees are paid by the user who creates the transaction. Fees are based on the size of the signed transaction (in bytes) and remain predictable and generally low. A commonly used standard fee is 0.00001 DASH per kB. Transactions offering higher fees

per byte may be prioritized by miners when block space is limited. While typical fees remain stable, they may increase during periods of elevated demand. CoinJoin transactions are usually free, aside from an occasional small fee applied randomly to mitigate spam.

The following applies to Tron:

Super Representatives earn 8 units of the native crypto-asset for each block they produce, while an additional 128 units per block are shared among all SRs and SR partners based on votes received. Voters obtain rewards through staking and voting, with SRs deducting a commission before distributing payouts. This incentive structure is intended to maintain active participation and reliable block production.

Transactions and smart-contract executions consume Bandwidth and Energy. Users can obtain these resources by staking or, if insufficient, by burning the native crypto-asset at fixed rates. Certain protocol actions such as becoming an SR candidate, issuing assets, creating accounts, or updating permissions carry dedicated execution fees, and optional costs apply for multi-signature transactions or memos.

While the protocol does not use slashing, resource-based penalties apply. Failed contract executions may result in increased Energy deductions, and the dynamic Energy model raises future costs for contracts that heavily consume network resources. These measures are intended to preserve system stability and prevent resource abuse.

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

2024-12-12

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

2025-12-12

S.8 Energy consumption

67500000.80459 kWh/a

S.9 Energy consumption sources and methodologies

For the calculation of energy consumptions, the so called 'bottom-up' approach is being used. The nodes are considered to be the central factor for the energy consumption of the network. These assumptions are made on the basis of empirical findings through the use of public information sites, open-source crawlers and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the client software. The energy consumption of the hardware devices was measured in certified test laboratories. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset of question in scope and we update the mappings regulary, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

To determine the energy consumption of a token, the energy consumption of the underlying blockchain networks is calculated first. A proportionate share of that energy use is then attributed to the token based on its activity level within the network (e.g. transaction volume, contract execution).

S.10 Renewable energy consumption

34.4781470956 %

S.11 Energy intensity

0.24714 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

27809.73446 tCO2e/a

S.14 GHG intensity

0.10182 kgCO2e

S.15 Key energy sources and methodologies

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

S.16 Key GHG sources and methodologies

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

https://ourworldindata.org/grapher/carbon-intensity-electricity Licenced under CC BY 4.0.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.