CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG V15WLZJMF

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified on 2026-05-26.

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 Bitcoin (BTC) crypto-asset to which this white paper refers is a crypto-asset other than an EMT or ART, native to the Bitcoin blockchain and available through the Lightning Network (a Layer 2 payment-channel network) as of 2026-05-18 and according to the DTI FFG shown in F.14. The first activity on the Bitcoin blockchain can be viewed on 2009-01-03 (block hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f, source: https://blockchair.com/bitcoin/block/0, accessed 2026-05-18). For the purposes of this white paper, the Lightning Network is referenced solely in accordance with the DTI FFG classification; it operates as a payment channel network built on top of the Bitcoin blockchain and does not constitute a separate or independent blockchain.

The crypto-asset was originally created by a pseudonymous individual or group known as "Satoshi Nakamoto". Its key characteristics include a fixed supply of 20,999,999.97690000 BTC, intended to make it a scarce asset, and it is used primarily as a store of value and medium of exchange. Bitcoin transactions are intended to be secured through a blockchain, which is intended to ensure they are secure, transparent, and immutable. The crypto-asset can be sent and received globally without intermediaries, making it censorship-resistant.

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers, including rights to ownership, profit participation, governance, or claims against any entity. Any functionalities accessible through the underlying technology are purely technical or operational in nature.

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

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

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

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

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

A.1 Name

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

A.2 Legal form

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

A.3 Registered address

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

Germany,

federal state of Hamburg.

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

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

A.6 Legal entity identifier

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

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

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

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

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

A.13 Business activity

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

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

A.14 Parent company business activity

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

A.15 Newly established

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

A.16 Financial condition for the past three years

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

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

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

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

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

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

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

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

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

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

A.17 Financial condition since registration

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

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

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

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

B.2 Name

The crypto-asset was originally created by a pseudonymous individual or group known as Satoshi Nakamoto, who published the Bitcoin white paper in 2008, outlining the core design of the project, and subsequently launched the network in 2009. As of the date of this white paper (2026-05-18), no issuing entity can be determined in a formal legal sense.

B.3 Legal form

Due to the nature of the decentralised network, the crypto-asset does not have a legal form as referred to in Article 6(1)(b) of Regulation (EU) 2023/1114.

B.4 Registered address

Due to the explaination given in field B.3 the crypto-asset issuer does not have a registered address.

Not applicable.

Not applicable.

B.5 Head office

As no issuing entity can be determined in a formal legal sense as of the date of this white paper, no head office address can be specified.

Not applicable.

Not applicable.

B.6 Registration date

Since the issuer of the crypto-asset did not register in a legal form there is no date of registration. The first block on the network was mined on 2009-01-03.

B.7 Legal entity identifier

Not applicable.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

The crypto-asset and its decentralized network are not operated by a legal entity and thus do not have a parent company.

B.10 Members of the management body

Identity	Function	Business Address
Not applicable	Not applicable	Not applicable

B.11 Business activity

The pseudonymous individual or group known as "Satoshi Nakamoto" has maintained its pseudonymity and thus there is no knowledge on the business or professional activity of the issuer. The last known activity on any platform was recorded on December 13th, 2010.

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, as Crypto Risk Metrics GmbH is not a trading platform.

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-asset white paper preparation

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

C.10 Members of the management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

Not applicable, as 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, as 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, as 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: "Bitcoin", Short name: "BTC, XBT" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-18).

D.2 Crypto-assets name

Long name: "Bitcoin" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-18).

D.3 Abbreviation

Short name: "BTC, XBT" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-05-18).

D.4 Crypto-asset project description

As described in the original white paper (https://bitcoin.org/bitcoin.pdf, accessed 10 March 2025), Bitcoin is intended to function as a decentralised, permissionless crypto-asset operating on a public, pseudonymous blockchain secured by the Proof-of-Work (PoW) consensus mechanism. Transactions are verified by miners who compete to solve cryptographic puzzles using the SHA-256 hashing algorithm, which is intended to ensure network security and immutability. Bitcoin's blockchain is structured as a linked chain of blocks, each containing a Merkle tree of transactions, with each block referencing the previous block's hash to maintain integrity. The supply is intended to be hard-capped at 20,999,999.97690000 BTC, enforced through a halving mechanism every 210,000 blocks (approximately four years), reducing block rewards and ensuring predictable issuance. Bitcoin's decentralised governance relies on Bitcoin Improvement Proposals (BIPs) and network consensus among full nodes, intending to prevent unilateral changes and reinforcing its censorship-resistant nature.

The Lightning Network is a supporting protocol built on top of the Bitcoin blockchain, which is intended to enable fast, low-cost, and scalable transactions.

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

Name of person	Type of person	Business address of person	Domicile of company
Satoshi Nakamoto (Pseudonym)	Other person involved in implementation	Cannot be determined	Cannot be determined

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

Past milestones:

1. Genesis Block (2009-01-03): The first Bitcoin block (Block 0) was mined by Satoshi Nakamoto on 2009-01-03, marking the creation of the Bitcoin network. The block contained an embedded message referencing the financial crisis then under way: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

2. First Bitcoin Transaction (2009-01-12): Satoshi Nakamoto sent 10 BTC to developer Hal Finney, making it the first recorded Bitcoin transaction.

3. Bitcoin Pizza Day (2010-05-22): Programmer Laszlo Hanyecz made the first real-world Bitcoin purchase, buying two pizzas for 10,000 BTC.

4. Segregated Witness (SegWit) Activation (August 2017): SegWit (BIP141) was activated to increase Bitcoin's transaction capacity by separating signature data from transaction data. This upgrade also laid the foundation for the Lightning Network, improving Bitcoin's scalability.

5. Taproot Upgrade (November 2021): Taproot (BIP341/BIP342) was activated, enhancing Bitcoin's privacy, efficiency and smart contract capabilities through Schnorr signatures. It improved multisig transactions and reduced transaction sizes, making Bitcoin more scalable and private.

6. Fourth Halving (April 2024): At block 840,000, the block reward was reduced from 6.25 BTC to 3.125 BTC, continuing Bitcoin's disinflationary issuance schedule.

Future milestones:

There is no formally defined roadmap for the Bitcoin network. Protocol changes are coordinated through the Bitcoin Improvement Proposal (BIP) process, an open mechanism through which any

participant may submit a formal document proposing changes, enhancements or additions to Bitcoin. Each proposal is subject to public discussion, technical review and, where applicable, miner and node signalling, and becomes part of the network only if it achieves broad consensus among developers, miners, node operators, and users. Any future milestones for the network will therefore be the outcome of community-driven decision-making rather than of decisions taken by a central party.

1. Covenants Soft Fork Discussion (2025 – ongoing): Discussions on introducing covenant functionality to Bitcoin have advanced, with proposals such as CHECKTEMPLATEVERIFY (BIP-119) and CHECKSIGFROMSTACK (BIP-348) remaining under active review by the developer community. As of the date of this white paper, no covenant-related soft fork has been activated on the Bitcoin mainnet, and any activation remains subject to network consensus.

2. Post-Quantum Cryptography Discussion (2026 – ongoing): Discussions on introducing quantum-resistant cryptography to Bitcoin have advanced.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. Future proposals may be modified, delayed, rejected, or discontinued through community-driven development and consensus processes. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the BTC crypto-asset for its holders.

D.9 Resource allocation

Not applicable. No specific project-level resource allocation attributable to a separate issuing entity has been identified or disclosed. This limits investors' ability to assess the funding and staffing dedicated specifically to this project.

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

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

As of 18 May 2026, approximately 20 million bitcoins have been mined, approaching the maximum supply limit of 20,999,999.97690000 BTC. However, not all mined bitcoins are actively available for trading. A significant number are considered lost due to forgotten private keys or dormant wallets, effectively reducing the circulating supply. Additionally, large holders, including institutions and governments, possess substantial amounts of bitcoin which may not be readily available in the market. Consequently, while the total number of mined bitcoins provides a general overview, the actual amount available for trading is lower, influenced by factors such as lost coins and holdings by large entities, which can have a negative impact on liquidity.

E.13 Targeted holders

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

E.14 Holder restrictions

Holder restrictions are subject to the rules applicable to the Crypto-Asset Service Provider, as well as to any additional restrictions such provider may impose.

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

The token is intended to be listed on the trading platform operated by Payward Global Solutions LTD ("Kraken"). Access to this platform depends on regional availability and user eligibility under

Kraken's terms and conditions. Investors should consult Kraken's official documentation to determine whether they meet the requirements for account creation and token trading.

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCA) but is neither classified as an electronic money token (EMT) nor an asset-referenced token (ART).

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

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

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

F.2 Crypto-asset functionality

The BTC crypto-asset is designed to function as a decentralised medium of exchange operating on a peer-to-peer network without reliance on a central intermediary. Transactions are validated and recorded on a public distributed ledger through a Proof-of-Work (PoW) consensus mechanism. The crypto-asset enables the transfer of value between participants and is primarily used for payment purposes and as a store of value.

The BTC crypto-asset does not confer ownership, profit participation, governance rights over any entity, or any form of economic entitlement. All functionalities are technical in nature and relate exclusively to interactions within the Bitcoin network. The actual usability of BTC depends on factors such as network stability, software implementation, development progress, and the operational conditions of the underlying distributed ledger, which are outside the control of token holders.

F.3 Planned application of functionalities

Due to the absence of an issuer and the existence of a decentralised consensus mechanism, there is no central authority with the power to define, plan or enforce future developments. Consequently, no planned functionalities can be defined or specified in a binding manner. While proposals for potential protocol changes exist in the form of Bitcoin Improvement Proposals (BIPs), no binding decision or implementation can be assumed, as any changes are subject to broad, decentralised consensus among network participants and no such consensus has been reached to date.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

The type of submission is MODI, which stands for "Modification".

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, native to the Bitcoin blockchain and available through the Lightning Network. The crypto-asset is fungible up to 8 digits after the decimal point. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics such as supply, demand, and liquidity in secondary markets.

F.7 Commercial name or trading name

Long name: "Bitcoin" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-05-18).

F.8 Website of the issuer

Not applicable.

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

2025-03-31

F.10 Publication date

2025-03-31

F.11 Any other services provided by the issuer

As no issuer is identified for the crypto-asset, 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

4H95J0R2X;K1NS41N51

F.14 Functionally fungible group digital token identifier

V15WLZJMF

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

LEI eligibility cannot be assessed, as no separate issuer is specified as a legal person in this white paper.

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

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

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

G.2 Exercise of rights and obligations

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

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

G.3 Conditions for modifications of rights and obligations

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

Adjustments to the protocol rules, node software, scripts, 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 was not available at the time of writing this white paper (2026-05-18).

G.5 Issuer retained crypto-assets

The following information concerns potential historical holdings attributed to Satoshi Nakamoto and is provided for informational purposes only.

According to various estimates, between approximately 600,000 and 1,500,000 bitcoin are believed to be held in wallets potentially controlled by an individual or group operating under the pseudonym Satoshi Nakamoto. This individual or group is generally regarded as the original developer of the Bitcoin protocol and the initiator of both the network and the corresponding crypto-asset.

The exact number of bitcoin held remains uncertain, as there is no verifiable information regarding the identity of the holder or holders, the specific wallet addresses or the effective control over these assets. Furthermore, it is legally unclear whether Satoshi Nakamoto, irrespective of any potential holdings, can be considered an issuer within the meaning of Regulation (EU) 2023/1114 (MiCA).

G.6 Utility token classification

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

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

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

G.8 Utility tokens redemption

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

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-05-18.

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

G.13 Supply adjustment mechanisms

Not applicable.

G.14 Token value protection schemes

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

G.15 Token value protection schemes description

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

G.16 Compensation schemes

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

G.17 Compensation schemes description

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

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DLT)

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

The following applies to Bitcoin:

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

1. Network protocols

- The crypto-asset follows a decentralised, peer-to-peer (P2P) protocol where nodes communicate using the "Bitcoin wire protocol" over TCP/IP.

- Bitcoin uses SHA-256 Proof-of-Work (PoW) to secure the network and validate transactions.

- Miners compete to find a valid nonce that satisfies the network's difficulty target.

- Transactions involving the crypto-asset use a stack-based scripting language for defining spending conditions.

2. Transaction and address standards

- Legacy format: P2PKH

- Script format: P2SH

- SegWit format: Bech32

- P2PKH – Standard transactions.

- P2SH – Enables complex scripts (e.g., multisig).

- P2WPKH/P2WSH – SegWit transactions reduce fees and fix malleability issues.

3. Blockchain data structure & block standards

- Transactions in each block are organised in a Merkle tree for efficient verification.

Each block contains:

- Block header: Previous block hash, Merkle root, timestamp, difficulty, nonce.

- Transactions: List of validated Bitcoin transactions.

- Block size limit: 1 MB (before SegWit), effectively ~4 MB with SegWit.

4. Upgrade & Improvement Standards

Bitcoin Improvement Proposals (BIPs)

- The crypto-asset community follows the BIP process for proposing protocol upgrades.

- Example BIPs:

- BIP32 – Hierarchical Deterministic (HD) wallets

- BIP39 – Mnemonic seed phrases for wallet backups

- BIP141 – Segregated Witness (SegWit)

- BIP340 – Schnorr signatures

- BIP341: Taproot

- BIP342: Tapscript

The following applies to the Lightning Network:

The Lightning Network is a Layer 2 scalability protocol built on top of the Bitcoin base layer, using bidirectional payment channels to enable instant, low-cost off-chain transactions that ultimately settle on Bitcoin Layer 1. It does not have its own consensus mechanism, native token, or global ledger; security is inherited from Bitcoin, while channel state is enforced through 2-of-2 multisignature outputs, cryptographic commitments, and Bitcoin Script. The following standards govern its operation:

1. Specification Framework: Basis of Lightning Technology (BOLT)

The Lightning Network does not rely on a single reference client; instead, interoperability across independent implementations (e.g. LND, Core Lightning, Eclair, LDK) is achieved through the BOLT specifications, a set of technical documents that define the protocol. The BOLT documents describe a layer-2 protocol for off-chain bitcoin transfer by mutual cooperation, relying on on-chain transactions for enforcement if necessary.

2. Channel and Transaction Standards

- Funding transactions: an on-chain 2-of-2 multisignature output (P2WSH or P2TR) locks the channel capacity on the Bitcoin base layer.

- Commitment transactions: mutually signed off-chain transactions that represent the current balance distribution between the two channel parties.

- Hashed Timelock Contracts (HTLCs): conditional payment primitives enabling trustless multi-hop routing across the network; funds either reach the destination via revelation of a cryptographic preimage or are refunded after a timelock expires.

3. Transport and Network Layer

Lightning nodes communicate peer-to-peer over TCP/IP (optionally via Tor), with all messages encrypted and authenticated using a customised variant of the Noise Protocol Framework (BOLT 8). Payment routing uses onion routing (BOLT 4) modelled on Sphinx, so that intermediate nodes only learn the previous and next hop, not the full payment path.

4. Upgrade Process

Lightning evolves through amendments to the BOLT specifications, with the convention that a new or modified BOLT is only formally adopted once at least two independent implementations have demonstrated interoperability. Application-level extensions that do not require full cross-implementation consensus are handled via bLIPs (Bitcoin Lightning Improvement Proposals).

H.3 Technology used

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

The following applies to Bitcoin:

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

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

3. Cryptographic Integrity: Bitcoin employs elliptic curve cryptography to validate and securely execute transactions, supporting the integrity of all transfers. The network uses the SHA-256 hashing algorithm within its Proof-of-Work consensus mechanism. Bitcoin addresses are derived through public-key cryptography using hashing mechanisms, including combinations of SHA-256 and RIPEMD-160. The crypto-asset uses ECDSA with the secp256k1 curve for key generation and digital signatures. In addition, Schnorr signatures were introduced through BIP340, enabling more efficient signature aggregation and verification, as well as supporting advanced transaction structures implemented through the Taproot upgrade.

The following applies to the Lightning Network:

The Lightning Network operates as a Layer 2 protocol that inherits its security from the Bitcoin base layer while enabling off-chain transfers between participants. Channel state is maintained as a mutually signed record between the two channel parties, with settlement on the Bitcoin blockchain occurring only on channel opening, closing, or dispute, supporting the integrity of all transfers without recording each payment on-chain.

Lightning relies on Bitcoin's elliptic curve cryptography for transaction validation, using ECDSA with the secp256k1 curve, and Schnorr signatures (BIP340) where channels are built on Taproot outputs. Channel funding is secured through 2-of-2 multisignature outputs on the Bitcoin base layer, while off-chain payments are secured by Hashed Timelock Contracts (HTLCs), which combine SHA-256 hash preimages with timelocks to enforce atomic, trustless routing across multiple hops. Interoperability across independent Lightning implementations is governed by the Basis of Lightning Technology (BOLT) specifications, which define channel construction, routing, transport encryption, and invoice encoding.

H.4 Consensus mechanism

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

The following applies to Bitcoin:

The crypto-asset's consensus mechanism is Proof-of-Work (PoW), which is intended to support network security and decentralisation. In PoW, miners calculate a hash of a proposed block header, which includes, among other data, a reference to the previous block, a Merkle root summarising the transactions included in the block, a timestamp, a difficulty target, and a nonce. The nonce and other variable fields may be adjusted until the resulting hash satisfies the applicable difficulty target. In computational terms, finding a suitable hash is difficult, while verifying it is comparatively simple.

When a miner identifies a valid block, the block is broadcast to other network nodes for verification. If the block complies with the applicable consensus rules, it may be added to the blockchain. The miner that produced the valid block may receive the applicable block reward and transaction fees.

Every 2,016 blocks, approximately every two weeks, the network automatically adjusts the difficulty target in order to maintain an average block interval of approximately 10 minutes. Bitcoin nodes follow the valid chain with the most cumulative Proof-of-Work, often referred to as the longest-chain rule. This mechanism is intended to make historical alteration of the blockchain difficult, as modifying past blocks would require recalculating the Proof-of-Work for those blocks and producing a valid chain with more cumulative Proof-of-Work than the honest network.

The following applies to the Lightning Network:

The Lightning Network does not have its own consensus algorithm and does not maintain a global ledger. It inherits consensus and security from the underlying Bitcoin base layer, with channel state

agreed bilaterally between the two channel participants and enforced on-chain through Bitcoin's Proof-of-Work consensus mechanism in the event of channel closure or dispute.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

The following applies to Bitcoin:

The crypto-asset's incentive mechanism is designed to encourage miners to secure the network and validate blocks. Miners may receive compensation through the block subsidy, consisting of newly issued BTC, and transaction fees associated with the transactions included in the block. The block subsidy is reduced by half approximately every 210,000 blocks, commonly referred to as the Bitcoin halving, which reduces the rate at which new BTC are created. This mechanism results in a maximum supply of approximately 21,000,000 BTC.

Transaction fees are paid by users to incentivise inclusion of their transactions in a block. Fees are dynamic and depend primarily on transaction size and demand for block space. During periods of high network activity, fees may increase as users compete for transaction inclusion. Conversely, when demand for block space is lower, fees may decrease. This fee market is intended to contribute to miner incentives as the block subsidy decreases over time.

The following applies to the Lightning Network:

The Lightning Network does not have its own block-based issuance mechanism and therefore does not provide a block subsidy or newly issued units as an incentive mechanism. Instead, participants may be compensated through routing fees. Nodes that forward payments along multi-hop routes may charge a fee, typically composed of a fixed base fee and a proportional component based on the amount routed. These fees are set by each node operator and are intended to compensate for the capital committed to channel liquidity and the operational cost of running a node.

In addition to routing fees, the protocol incorporates a penalty, or revocation, mechanism intended to align incentives between channel counterparties. If a counterparty broadcasts a revoked or outdated channel state to the Bitcoin base layer, the honest party may use the corresponding revocation secret to claim the channel funds made available under the applicable penalty transaction. This is intended to deter fraudulent channel closures and to support the integrity of off-chain state without reliance on a separate block-based consensus mechanism. Where the honest party is offline, third-party watchtower services may be used to monitor the Bitcoin blockchain and enforce the penalty mechanism on its behalf.

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 centralised exchanges (CEXs) or decentralised exchanges (DEXs). Trading volumes may at times be low, order books thin, or liquidity concentrated

on a single venue. In such conditions, buy or sell orders may not be executed in full or may be executed only at a less favourable price, resulting in slippage.

Volatility: The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the crypto-asset at or close to a previously observed price, even 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 centralised or decentralised trading venues, liquidity providers, brokers, custodians, or technical integrators. If any of these counterparties fail to perform, suspend their services, or apply internal restrictions, the trading, deposit, or withdrawal of the crypto-asset on the 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 recognised 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

Interpretative note for this section: The risk factors set out in this Part I.2 follow the structure of the applicable MiCA white paper template for crypto-assets other than asset-referenced tokens or e-money tokens under Title II of MiCA, including references to issuer-related risks. For the purposes of this Part I.2, references to an "issuer", "issuer-related risks", or similar terms are to be read in line with the definition of "issuer" under MiCA, including any natural or legal person, or other undertaking, that issues crypto-assets. Where this white paper does not specify a separate issuer, the relevant risk descriptions should be understood as referring, as applicable, to persons, entities, undertakings, arrangements, or governance structures that may materially influence the crypto-asset or the related project. This may include, for example, foundations, core contributor entities, developers, maintainers, governance participants, or other relevant project-related actors, to the extent such information is available.

1. Absence or insolvency of an identifiable issuer

Where an identifiable issuer exists, that issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, legal or regulatory developments, or external shocks, including pandemics or armed conflicts. In such a case, ongoing development, support, communication, or governance of the crypto-asset project may be reduced, suspended, or discontinued, potentially affecting the viability, availability, market acceptance, or tradability of the crypto-asset.

2. Legal and regulatory risks

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

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

The crypto-asset 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

Interpretative note for this section: The risk factors set out in this Part I.4 follow the structure of the applicable MiCA white paper template for crypto-assets other than asset-referenced tokens or e-money tokens under Title II of MiCA, including references to issuer-related risks. For the purposes of this Part I.4, references to an “issuer”, “issuer-related risks”, or similar terms are to be read in line with the definition of “issuer” under MiCA, including any natural or legal person, or other undertaking, that issues crypto-assets. Where this white paper does not specify a separate issuer, the relevant risk descriptions should be understood as referring, as applicable, to persons, entities, undertakings, arrangements, or governance structures that may materially influence the crypto-asset or the related project. This may include, for example, foundations, core contributor entities, developers, maintainers, governance participants, or other relevant project-related actors, to the extent such information is available.

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 Bitcoin blockchain and, where applicable, the Lightning Network. Network congestion, outages, or protocol errors may temporarily or permanently disrupt on-chain transactions or Layer 2 transfers. Extended downtime or degradation in network performance can affect trading, settlement, or usability of the crypto-asset.

2. Protocol and software vulnerability risk

The protocol rules, scripts, software implementations, or related technical components that define the crypto-asset's parameters or govern its transfers may contain coding errors or security vulnerabilities. Exploitation of such weaknesses can result in unintended consequences, including loss of funds or disruption of network functionality. Even after extensive peer review and community auditing, undetected vulnerabilities may persist, particularly given the long-standing and deeply embedded nature of the 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 Bitcoin protocol or Lightning Network specifications (e.g. network upgrades, soft forks, or BOLT specification revisions) 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 Bitcoin or Lightning networks. 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: The Bitcoin network may be subject to denial-of-service (DoS) attacks, 51% attacks, or other exploits targeting the proof-of-work consensus mechanism. These can delay transactions, compromise finality, or disrupt the accurate recording of transfers. The Lightning Network may additionally be exposed to channel-jamming attacks, routing failures, or other Layer 2 specific vulnerabilities.

Centralisation Concerns: Despite the decentralised design of the Bitcoin protocol, a high concentration of mining hashrate among a small number of mining pools may increase the risk of collusion, censorship, or coordinated network disruption. Similar concerns may apply to the Lightning Network where routing capacity is concentrated among a limited number of well-funded nodes. These factors can affect the resilience and operational reliability of the crypto-asset.

5. Bridge and interoperability risk

Where the crypto-asset is represented on networks other than the Bitcoin blockchain or the Lightning Network through third-party infrastructure such as bridges, wrapped representations, or synthetic instruments, vulnerabilities in such external protocols, validator sets, or locking mechanisms may result in loss, duplication, or misrepresentation of assets. These risks arise outside the native Bitcoin and Lightning scope and depend on the integrity of the third-party systems concerned. Exploits or technical failures in such systems can impact circulating supply, ownership claims, or token fungibility across chains.

6. Forking and protocol-upgrade risk

Network upgrades or disagreements among node operators or miners 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 Layer 2 protocols, wrapped representations, or synthetic instruments may alter the transaction economics of the underlying crypto-asset. Changes in network transaction fees, Lightning routing fees, demand for block space, or utility may reduce usage and weaken both the economic function and perceived value of the crypto-asset within its ecosystem.

8. Spam and network-efficiency risk

High volumes of low-value ("dust") or automated transactions may congest the network, slow block propagation, inflate ledger size, and raise network transaction fees. 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 Bitcoin or Lightning networks, service outages, malicious compromises, or domain expiries affecting these interfaces may block access to the crypto-asset, even while the underlying networks themselves remain 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 of the Bitcoin network is widely regarded as decentralised, certain operational layers, such as mining pool concentration, software development repositories, or Lightning Network routing capacity, may exhibit higher degrees of centralisation. This disconnect between general perception and structural reality can give rise to regulatory scrutiny or reputational concerns, particularly where claims of full decentralisation are made without substantiation.

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the crypto-asset

Bitcoin

S.4 Consensus Mechanism

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

The following applies to Bitcoin:

The crypto-asset's consensus mechanism is Proof-of-Work (PoW), which is intended to support network security and decentralisation. In PoW, miners calculate a hash of a proposed block header, which includes, among other data, a reference to the previous block, a Merkle root summarising the transactions included in the block, a timestamp, a difficulty target, and a nonce. The nonce and other variable fields may be adjusted until the resulting hash satisfies the applicable difficulty target. In computational terms, finding a suitable hash is difficult, while verifying it is comparatively simple.

When a miner identifies a valid block, the block is broadcast to other network nodes for verification. If the block complies with the applicable consensus rules, it may be added to the blockchain. The miner that produced the valid block may receive the applicable block reward and transaction fees.

Every 2,016 blocks, approximately every two weeks, the network automatically adjusts the difficulty target in order to maintain an average block interval of approximately 10 minutes. Bitcoin nodes follow the valid chain with the most cumulative Proof-of-Work, often referred to as the longest-chain rule. This mechanism is intended to make historical alteration of the blockchain difficult, as modifying past blocks would require recalculating the Proof-of-Work for those blocks and producing a valid chain with more cumulative Proof-of-Work than the honest network.

The following applies to the Lightning Network:

The Lightning Network does not have its own consensus algorithm and does not maintain a global ledger. It inherits consensus and security from the underlying Bitcoin base layer, with channel state agreed bilaterally between the two channel participants and enforced on-chain through Bitcoin's Proof-of-Work consensus mechanism in the event of channel closure or dispute.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is native to the Bitcoin blockchain and transferable through the Lightning Network, following the standards described below.

The following applies to Bitcoin:

The crypto-asset's incentive mechanism is designed to encourage miners to secure the network and validate blocks. Miners may receive compensation through the block subsidy, consisting of newly issued BTC, and transaction fees associated with the transactions included in the block. The block subsidy is reduced by half approximately every 210,000 blocks, commonly referred to as the Bitcoin

halving, which reduces the rate at which new BTC are created. This mechanism results in a maximum supply of approximately 21,000,000 BTC.

Transaction fees are paid by users to incentivise inclusion of their transactions in a block. Fees are dynamic and depend primarily on transaction size and demand for block space. During periods of high network activity, fees may increase as users compete for transaction inclusion. Conversely, when demand for block space is lower, fees may decrease. This fee market is intended to contribute to miner incentives as the block subsidy decreases over time.

The following applies to the Lightning Network:

The Lightning Network does not have its own block-based issuance mechanism and therefore does not provide a block subsidy or newly issued units as an incentive mechanism. Instead, participants may be compensated through routing fees. Nodes that forward payments along multi-hop routes may charge a fee, typically composed of a fixed base fee and a proportional component based on the amount routed. These fees are set by each node operator and are intended to compensate for the capital committed to channel liquidity and the operational cost of running a node.

In addition to routing fees, the protocol incorporates a penalty, or revocation, mechanism intended to align incentives between channel counterparties. If a counterparty broadcasts a revoked or outdated channel state to the Bitcoin base layer, the honest party may use the corresponding revocation secret to claim the channel funds made available under the applicable penalty transaction. This is intended to deter fraudulent channel closures and to support the integrity of off-chain state without reliance on a separate block-based consensus mechanism. Where the honest party is offline, third-party watchtower services may be used to monitor the Bitcoin blockchain and enforce the penalty mechanism on its behalf.

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

2024-03-22

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

2025-03-22

S.8 Energy consumption

174523635953.08917 kWh/a

S.9 Energy consumption sources and methodologies

For the calculation of energy consumption, the so-called "top-down" approach is used, within which an economic calculation of the miners is assumed. Miners are persons or devices that actively participate in the Proof-of-Work consensus mechanism. Miners are considered to be the central factor in the energy consumption of the network. Hardware is pre-selected based on the consensus mechanism's hash algorithm: SHA-256. A current profitability threshold is determined on the basis of the revenue and cost structure for mining operations. Only hardware above the profitability threshold is considered for the network. The energy consumption of the network can be determined by taking into account the distribution of hardware, the efficiency levels for operating the hardware, and on-chain information regarding the miners' revenue opportunities. If significant use of merge mining is known, this is taken into account.

For the calculation of the corresponding indicators, the additional energy consumption and the transactions of the Lightning Network have also been taken into account, as this reflects the categorisation of the Digital Token Identifier Foundation for the respective functionally fungible group ("FFG") relevant for this reporting.

S.10 Renewable energy consumption

34.4781471084 %

S.11 Energy intensity

15.47710 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

71903050.62182 tCO2e/a

S.14 GHG intensity

6.37650 kgCO2e

S.15 Key energy sources and methodologies

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

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

S.16 Key GHG sources and methodologies

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

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.