CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG RQPCRN3VN

Preamble

00. Table of Contents

01. Date of notification 11

02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114 11

03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114 11

04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114 11

05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114 .. 11

06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114 12

Summary 12

07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114 12

08. Characteristics of the crypto-asset 12

09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability 13

10. Key information about the offer to the public or admission to trading 13

Part A – Information about the offeror or the person seeking admission to trading 13

A.1 Name 13

A.2 Legal form 13

A.3 Registered address 14

A.4 Head office 14

A.5 Registration date 14

A.6 Legal entity identifier 14
A.7 Another identifier required pursuant to applicable national law 14
A.8 Contact telephone number 14
A.9 E-mail address 14
A.10 Response time (Days) 14
A.11 Parent company 14
A.12 Members of the management body 14
A.13 Business activity 15
A.14 Parent company business activity 15
A.15 Newly established 15
A.16 Financial condition for the past three years 15
A.17 Financial condition since registration 16
Part B – Information about the issuer, if different from the offeror or person seeking admission to trading 16
B.1 Issuer different from offeror or person seeking admission to trading 16
B.2 Name 16
B.3 Legal form 16
B.4. Registered address 16
B.5 Head office 16
B.6 Registration date 16
B.7 Legal entity identifier 16
B.8 Another identifier required pursuant to applicable national law 16
B.9 Parent company 17
B.10 Members of the management body 17
B.11 Business activity 17

B.12 Parent company business activity 17

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 17

C.1 Name 17

C.2 Legal form 17

C.3 Registered address 17

C.4 Head office 17

C.5 Registration date 17

C.6 Legal entity identifier 18

C.7 Another identifier required pursuant to applicable national law 18

C.8 Parent company 18

C.9 Reason for crypto-Asset white paper Preparation 18

C.10 Members of the Management body 18

C.11 Operator business activity 18

C.12 Parent company business activity 18

C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 18

C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 18

Part D – Information about the crypto-asset project 19

D.1 Crypto-asset project name 19

D.2 Crypto-assets name 19

D.3 Abbreviation 19

D.4 Crypto-asset project description 19

D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project 19

D.6 Utility Token Classification 20

D.7 Key Features of Goods/Services for Utility Token Projects 20

D.8 Plans for the token 20

D.9 Resource allocation 20

D.10 Planned use of Collected funds or crypto-Assets 20

Part E – Information about the offer to the public of crypto-assets or their admission to trading 21

E.1 Public offering or admission to trading 21

E.2 Reasons for public offer or admission to trading 21

E.3 Fundraising target 21

E.4 Minimum subscription goals 21

E.5 Maximum subscription goals 21

E.6 Oversubscription acceptance 22

E.7 Oversubscription allocation 22

E.8 Issue price 22

E.9 Official currency or any other crypto-assets determining the issue price 22

E.10 Subscription fee 22

E.11 Offer price determination method 22

E.12 Total number of offered/traded crypto-assets 22

E.13 Targeted holders 22

E.14 Holder restrictions 23

E.15 Reimbursement notice 23

E.16 Refund mechanism 23
E.17 Refund timeline 23
E.18 Offer phases 23
E.19 Early purchase discount 23
E.20 Time-limited offer 23
E.21 Subscription period beginning 23
E.22 Subscription period end 24
E.23 Safeguarding arrangements for offered funds/crypto- Assets 24
E.24 Payment methods for crypto-asset purchase 24
E.25 Value transfer methods for reimbursement 24
E.26 Right of withdrawal 24
E.27 Transfer of purchased crypto-assets 24
E.28 Transfer time schedule 24
E.29 Purchaser's technical requirements 24
E.30 Crypto-asset service provider (CASP) name 25
E.31 CASP identifier 25
E.32 Placement form 25
E.33 Trading platforms name 25
E.34 Trading platforms Market identifier code (MIC) 25
E.35 Trading platforms access 25
E.36 Involved costs 25
E.37 Offer expenses 25
E.38 Conflicts of interest 25
E.39 Applicable law 26

E.40 Competent court 26

Part F – Information about the crypto-assets 26

F.1 Crypto-asset type 26

F.2 Crypto-asset functionality 26

F.3 Planned application of functionalities 27

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 27

F.4 Type of crypto-asset white paper 27

F.5 The type of submission 27

F.6 Crypto-asset characteristics 27

F.7 Commercial name or trading name 27

F.8 Website of the issuer 27

F.9 Starting date of offer to the public or admission to trading 27

F.10 Publication date 27

F.11 Any other services provided by the issuer 28

F.12 Language or languages of the crypto-asset white paper 28

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 28

F.14 Functionally fungible group digital token identifier, where available 28

F.15 Voluntary data flag 28

F.16 Personal data flag 28

F.17 LEI eligibility 28

F.18 Home Member State 28

F.19 Host Member States 28

Part G – Information on the rights and obligations attached to the crypto-assets 29

G.1 Purchaser rights and obligations 29

G.2 Exercise of rights and obligations 29

G.3 Conditions for modifications of rights and obligations 29

G.4 Future public offers 29

G.5 Issuer retained crypto-assets 29

G.6 Utility token classification 30

G.7 Key features of goods/services of utility tokens 30

G.8 Utility tokens redemption 30

G.9 Non-trading request 30

G.10 Crypto-assets purchase or sale modalities 30

G.11 Crypto-assets transfer restrictions 30

G.12 Supply adjustment protocols 30

G.13 Supply adjustment mechanisms 30

G.14 Token value protection schemes 31

G.15 Token value protection schemes description 31

G.16 Compensation schemes 31

G.17 Compensation schemes description 31

G.18 Applicable law 31

G.19 Competent court 31

Part H – information on the underlying technology 31

H.1 Distributed ledger technology (DTL) 31

H.2 Protocols and technical standards 32

H.3 Technology used 33

H.4 Consensus mechanism 34

H.5 Incentive mechanisms and applicable fees 37

H.6 Use of distributed ledger technology 39

H.7 DLT functionality description 39

H.8 Audit 40

H.9 Audit outcome 40

Part I – Information on risks 40

I.1 Offer-related risks 40

I.2 Issuer-related risks 42

I.3 Crypto-assets-related risks 43

I.4 Project implementation-related risks 48

I.5 Technology-related risks 48

I.6 Mitigation measures 50

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts 50

J.1 Adverse impacts on climate and other environment-related adverse impacts 50

S.1 Name 50

S.2 Relevant legal entity identifier 50

S.3 Name of the cryptoasset 51

S.4 Consensus Mechanism 51

S.5 Incentive Mechanisms and Applicable Fees 54

S.6 Beginning of the period to which the disclosure relates 56

S.7 End of the period to which the disclosure relates 56

S.8 Energy consumption 56

S.9 Energy consumption sources and methodologies 56

S.10 Renewable energy consumption 56

S.11 Energy intensity 56

S.12 Scope 1 DLT GHG emissions – Controlled 57

S.13 Scope 2 DLT GHG emissions – Purchased 57

S.14 GHG intensity 57

S.15 Key energy sources and methodologies 57

S.16 Key GHG sources and methodologies 57

01. Date of notification

2025-08-25

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

The token has no utility other than being holdable and transferable and can not be exchanged for any goods or services at the time of writing this white paper (2025-08-16).

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 MAGIC INTERNET MONEY tokens referred to in this white paper are crypto-assets other than EMTs and ARTs, and are issued on the Solana blockchain and as a Rune (2025-08-16 and according to DTI FFG shown in F.14).

The creation of Runes tooks place on 2024-04-30 with 21,000,000,000 token (see transaction: https://ordiscan.com/rune/MAGICINTERNETMONEY).

The first activity on Solana can be identified on 2025-03-03 (see transaction: https://solscan.io/tx/4x7odDkDA9nkhpWECNGXV64YxCH68mBdExJsce4hjA8aXTfcAjC87B1LCU5xHoavWmDTxjAK7s9GWfQQFcU7w2sb).

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

Not applicable.

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. If a CASP wishes to use this white paper, inquiries can be made under info@crypto-risk-metrics.com.

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

A.1 Name

Crypto Risk Metrics GmbH

A.2 Legal form

2HBR

A.3 Registered address

DE, Lange Reihe 73, 20099 Hamburg, Germany

A.4 Head office

Not applicable.

A.5 Registration date

2018-12-03

A.6 Legal entity identifier

39120077M9TG0O1FE242

A.7 Another identifier required pursuant to applicable national law

Crypto Risk Metrics GmbH is registered with the commercial register in the the city of Hamburg, Germany, under number HRB 154488.

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

030

A.11 Parent company

Not applicable.

A.12 Members of the management body

Name	Position	Address
Tim Zölitz	Chairman	Lange Reihe 73, 20099 Hamburg, Germany

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider, who supports regulated entities in the fulfillment of their regulatory requirements. In this regard, Crypto Risk Metrics GmbH acts as a data-provider for ESG-data according to article 66 (5). Due to the regulations laid out in article 5 (4) 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 at providing central services for crypto-asset white papers in order to minimize market confusion due to conflicting white papers for the same asset.

A.14 Parent company business activity

Not applicable.

A.15 Newly established

Crypto Risk Metrics GmbH has been etablished since 2018 and is therefore not newly established (i. e. older than three years).

A.16 Financial condition for the past three years

Crypto Risk Metrics GmbH's profit after tax for the last three financial years are as follows:

2024 (unaudited): negative 50.891,81 EUR

2023 (unaudited): negative 27.665,32 EUR

2022: 104.283,00 EUR.

As 2023 and 2024 were the years building Software for the MiCAR-Regulation which was not yet in place, revenue streams from these investments are expeted to be generated in 2025.

A.17 Financial condition since registration

This point would only be applicable if the company were newly established and the financial conditions for the past three years had not been provided in the bulletpoint before.

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

B.2 Name

The token does not appear to be issued by a formal company or foundation in the traditional sense. Instead, it follows a decentralized, community-driven approach common in the meme coin space.

B.3 Legal form

Could not be found while drafting this white paper (2025-08-16).

B.4. Registered address

Could not be found while drafting this white paper (2025-08-16).

B.5 Head office

Could not be found while drafting this white paper (2025-08-16).

B.6 Registration date

Could not be found while drafting this white paper (2025-08-16).

B.7 Legal entity identifier

Could not be found while drafting this white paper (2025-08-16).

B.8 Another identifier required pursuant to applicable national law

Could not be found while drafting this white paper (2025-08-16).

B.9 Parent company

Could not be found while drafting this white paper (2025-08-16).

B.10 Members of the management body

Could not be found while drafting this white paper (2025-08-16).

B.11 Business activity

Could not be found while drafting this white paper (2025-08-16).

B.12 Parent company business activity

Could not be found while drafting this white paper (2025-08-16).

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.

C.2 Legal form

Not applicable.

C.3 Registered address

Not applicable.

C.4 Head office

Not applicable.

C.5 Registration date

Not applicable.

C.6 Legal entity identifier

Not applicable.

C.7 Another identifier required pursuant to applicable national law

Not applicable.

C.8 Parent company

Not applicable.

C.9 Reason for crypto-Asset white paper Preparation

Not applicable.

C.10 Members of the Management body

Not applicable.

C.11 Operator business activity

Not applicable.

C.12 Parent company business activity

Not applicable.

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.

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.

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: MAGIC INTERNET MONEY, Short Name: Bitcoin according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-08-16).

D.2 Crypto-assets name

See F.13.

D.3 Abbreviation

See F.13.

D.4 Crypto-asset project description

MAGIC INTERNET MONEY is a meme-driven crypto-asset launched in April 2024 on the Bitcoin blockchain. It was inspired by the Bitcoin Wizard Magic Internet Money meme from 2013 r/bitcoin subreddit ad.

Unlike traditional projects, MAGIC INTERNET MONEY is not backed by a formal company, foundation, or legal entity. It emerged as a celebration of Bitcoin culture and the meme that contributed to Bitcoin's early reddit adoption in 2013.

MAGIC INTERNET MONEY has no official roadmap, utility, or governance structure. Its value and relevance are entirely driven by the strength of community sentiment and the symbolic weight of the story behind it.

In contrast to structured crypto ventures, MAGIC INTERNET MONEY operates as a pure meme token with no guarantees, rights, or formal affiliations. It represents the unpredictable, often emotional nature of meme-based assets within the crypto ecosystem.

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

At the time of writing this white paper (2025-08-16), there is no identifiable central team or advisors. Community members contribute voluntarily through open forums and

social media channels. There are no formal development teams, advisors, or service providers under contract.

D.6 Utility Token Classification

The token does not classify as a utility token.

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

Not applicable.

D.8 Plans for the token

At the time of writing this white paper (2025-06-16), no future plans for the crypto-asset were to be found.

D.9 Resource allocation

At the time of writing this white paper (2025-08-17), no officially published information on this matter can be found by the issuer.

The temporary token distribution can be traced on-chain, on Solana: https://solscan.io/token/M1M6sdffCs3ozzhpRveweRCWdZhxth4mvVujPtYEC3h#holders

The investor must be aware that a public address cannot necessarily be assigned to a single person or entity, which limits the ability to determine exact economic influence or future actions. Token distribution changes can negatively impact the investor.

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

Not applicable, as this white paper was drawn up for the admission to trading and not for collecting funds 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) on any Crypto Asset Service Providers platform that has obtained the written consent of Crypto Risk Metrics GmbH as the person drafting this white paper.

E.2 Reasons for public offer or admission to trading

As already stated in A.13, Crypto Risk Metrics GmbH aims to provide central services to draw up crypto-asset white papers in accordance to COMMISSION IMPLEMENTING REGULATION (EU) 2024/2984. These services are offered in order to minimize market confusion due to conflicting white papers for the same asset drawn up from different Crypto Asset Service Providers. As of now, such a scenario seems highly likely as a Crypto Asset Service Provider who drew up a crypto-asset white paper and admitted the respective token in the Union has no incentive to give his written consent to another Crypto Asset Service Provider according to Article 5 (4 b) of the REGULATION (EU) 2023/1114 to use the white paper for his regulatory obligations, as this would 1. strenghthen the market-positioning of the other Crypto Asset Service Provider (who is most likely a competitor) and 2. also entail liability risks.

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

E.10 Subscription fee

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

E.11 Offer price determination method

Once the token is admitted to trading its price will be determined by demand (buyers) and supply (sellers).

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

As stated on the website https://ordiscan.com/rune/MAGICINTERNETMONEY and https://solscan.io/token/M1M6sdffCs3ozzhpRveweRCWdZhxth4mvVujPtYEC3h, accessed 2025-08-20) a total of 21,000,000,000 tokens were minted.

E.13 Targeted holders

ALL

E.14 Holder restrictions

The Holder restrictions are subject to the rules applicable to the Crypto Asset Service Provider as well as additional restrictions the Crypto Asset Service Providers might set in force.

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

E.24 Payment methods for crypto-asset purchase

The payment methods are subject to the respective capabilities of the Crypto Asset Service Provider listing the crypto-asset.

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

The transfer of purchased crypto-assets are subject to the respective capabilities of the Crypto Asset Service Provider listing the crypto-asset.

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

The technical requirements that the purchaser is required to fulfil to hold the crypto-assets of purchased crypto-assets are subject to the respective capabilities of the Crypto Asset Service Provider listing the crypto-asset.

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

Not applicable.

E.31 CASP identifier

Not applicable.

E.32 Placement form

Not applicable.

E.33 Trading platforms name

The trading on all MiCAR-compliant trading platforms is sought.

E.34 Trading platforms Market identifier code (MIC)

Not applicable.

E.35 Trading platforms access

This depends on the trading platform listing the asset.

E.36 Involved costs

This depends on the trading platform listing the asset. Furthermore, costs may occur for making transfers out of the platform (i. e. "gas costs" for blockchain network use that may exceed the value of the crypto-asset itself).

E.37 Offer expenses

Not applicable, as this crypto-asset white paper concerns the admission to trading and not the offer of the token to the public.

E.38 Conflicts of interest

MiCAR-compliant Crypto Asset Service Providers shall have strong measurements in place in order to manage conflicts of interests. Due to the broad audience this white-paper is adressing, potential investors should always check the conflicts of Interest policy of their respective counterparty.

E.39 Applicable law

Not applicable, as it is referred to on "offer to the public" and in this white-paper, the admission to trading is sought.

E.40 Competent court

Not applicable, as it is referred to on "offer to the public" and in this white-paper, the admission to trading is sought.

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 (MiCAR) but does not qualify 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 supported by a stabilization mechanism. It is neither pegged to any fiat currency nor backed by any external assets, distinguishing it clearly from EMTs and ARTs.

Furthermore, the crypto-asset is not categorized 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

There is none, other than the ability to hold and transfer the crypto-asset.

F.3 Planned application of functionalities

All functionalities referred to in F.2 have already been applied. There were no statements to be found to further functionalities for the token while drafting this white paper (2025-06-16).

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 white paper submission type is "NEWT", which stands for new token.

F.6 Crypto-asset characteristics

The tokens are crypto-assets other than EMTs and ARTs, which are available on the Solana and Bitcoin (as Rune) blockchain. The tokens are fungible (up to 2 digits on Solana after the decimal point), and a total of 21,000,000,000 have already been issued. The tokens are a digital representation of value, and have no inherent rights attached as well as no intrinsic utility.

F.7 Commercial name or trading name

See F.13.

F.8 Website of the issuer

https://magicinternetmoney.party/

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

2025-09-22

F.10 Publication date

2025-09-22

F.11 Any other services provided by the issuer

It is not possible to exclude a possibility that the issuer of the token provides or will provide other services not covered by Regulation (EU) 2023/1114 (i.e. MiCAR).

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

GXWQQ3LPH; JQDK5K0P1

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

RQPCRN3VN

F.15 Voluntary data flag

Mandatory.

F.16 Personal data flag

The white paper does contain personal data.

F.17 LEI eligibility

The issuer should be eligible for a Legal Entity Identifier.

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

There are no rights or obligations attached for/of the purchaser.

G.2 Exercise of rights and obligations

As the token grants neither rights nor obligations, there are no procedures and conditions for the exercise of these rights applicable.

G.3 Conditions for modifications of rights and obligations

As the token grants neither rights nor obligations, there are no conditions under which the rights and obligations may be modified applicable. An adjustment of the technical infrastructure necessary to exercise the promised governance rights, declining functionality due to dilution, changing rights within the voting platforms, and all other adverse effects for investors may occur at any time.

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 (2025-08-15).

G.5 Issuer retained crypto-assets

At the time of writing this white paper (2025-08-17), no officially published information on the planned token distribution can be found by the issuer. According to the official documentation, no assets are held by the team or insiders (https://magicinternetmoney.party/#tokenomics, accessed 2025-08-20). However, this information cannot be independently verified and must therefore be viewed critically.

The temporary token distribution can be traced on-chain, on Solana: https://solscan.io/token/M1M6sdffCs3ozzhpRveweRCWdZhxth4mvVujPtYEC3h#holders

The investor must be aware that a public address cannot necessarily be assigned to a single person or entity, which limits the ability to determine exact economic influence or future actions. Token distribution changes can negatively impact the investor.

G.6 Utility token classification

No

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

Not applicable.

G.8 Utility tokens redemption

Not applicable.

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 support admission to trading and not for the initial offer to the public.

G.11 Crypto-assets transfer restrictions

The crypto-assets as such do not have any transfer restrictions and are generally freely transferable. The Crypto Asset Service Providers can impose their own restrictions in agreements they enter with their clients. The Crypto Asset Service Providers may impose restrictions to buyers and sellers in accordance with applicable laws and internal policies and terms.

G.12 Supply adjustment protocols

No, there are no fixed protocols that can increase or decrease the supply implemented as of 2025-08-19. Furthermore, the supply cannot be increased because mint authority for the token was permanently forfeited. Tokens can be burned by any user.

G.13 Supply adjustment mechanisms

The project states that it has a fixed token limit and cannot generate any further assets (https://magicinternetmoney.party/#tokenomics, accessed 2025-08-20). The asset (Rune) is also declared as no longer mintable: (https://ordiscan.com/rune/MAGICINTERNETMONEY, accessed 2025-08-20).

The mint authority on Solana (the entity who can create new tokens of that crypto-asset), as stated in the mint's data account, has the potential right to change the supply of the crypto-assets. However, since the mint authority was forfeited, it should not be possible to increase the token supply, however the whole data account could be updated which then in turn could lead to a situation that total suppy could be altered again.

G.14 Token value protection schemes

No, the token does not have value protection schemes.

G.15 Token value protection schemes description

Not applicable.

G.16 Compensation schemes

No, the token does not have compensation schemes.

G.17 Compensation schemes description

Not applicable.

G.18 Applicable law

Applicable law likely depends on the location of any particular transaction with the token.

G.19 Competent court

Competent court likely depends on the location of any particular transaction with the token.

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

See F.13.

H.2 Protocols and technical standards

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana and Bitcoin (via so called "Runes"). In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Bitcoin/Runes:

The token was created using the Runes Protocol, a fungible token standard on the Bitcoin blockchain. Unlike established smart-contract-based frameworks, Runes embed token data directly into Bitcoin transactions via Unspent Transaction Output (UTXO), enabling issuance, transfer, and balance tracking without an external virtual machine. This approach ensures that tokens exist natively within the Bitcoin ledger, but it also relies on a technical standard that is still experimental, with limited operational history.

The following applies to Solana:

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

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

Core functions of the Token Program:

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

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

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

transfer() → Transfers tokens between accounts

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

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

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

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

H.3 Technology used

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana and Bitcoin (via so called "Runes"). In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Bitcoin/Runes:

The tokens are created through the Runes Protocol, which embeds token balances and transfers directly into Bitcoin transactions. This approach does not involve a separate smart contract layer but relies on the Bitcoin ledger itself.

As the Runes Protocol is novel and only recently introduced, it lacks a proven operational history, creating uncertainty regarding scalability, compatibility with wallets and exchanges, and resilience under stressed market conditions. Security ultimately depends on Bitcoin's proof-of-work consensus and private key management, but the Runes Protocol remains relatively untested. Security ultimately depends on Bitcoin's proof-of-work consensus and private key management, while the functionality of Runes

is fully dependent on Bitcoin's underlying technology, including its inherent limitations with respect to scalability and transaction throughput.

The following applies to Solana:

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

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

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

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

Security Protocols for Asset Custody and Transactions:

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

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

H.4 Consensus mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana and Bitcoin (via so called "Runes"). In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Bitcoin/Runes:

The consensus mechanism from Bitcoin is Proof-of-Work (PoW), which intends to provide security and decentralization. In PoW, miners calculate a hash function of their respective newly proposed blocks, a summary of the previous block and a nonce variable. The nonce variable is adjusted until the result of the hash function satisfies a predefined difficulty target. In a computational sense it is very difficult to find a suitable nonce, but it is very easy to verify it. When a miner finds a suitable nonce, the new block including the nonce is broadcast to other nodes to be verified. Verified blocks are then added to the blockchain. The miner who made the block is rewarded. Every 2016 blocks (around 2 Weeks) the network automatically adjusts the difficulty target, to maintain a block time of around 10 minutes. The network follows the longest chain rule, where nodes always consider the longest valid chain as the correct version.

The following applies to Solana:

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

Core Concepts

1. Proof of History (PoH):

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

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

2. Proof of Stake (PoS):

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

selected to validate transactions and produce new blocks.

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

cryptographic clock for the network.

3. Block Production:

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

4. Consensus and Finalization:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

H.5 Incentive mechanisms and applicable fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana and Bitcoin (via so called "Runes"). In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Bitcoin/Runes:

The incentive mechanism of Bitcoin is designed to encourage miners to secure the network and validate transactions. Miners are rewarded with block rewards (newly minted Bitcoins) and transaction fees for every block that they add to the chain. The block reward is halved approximately every four years in an event known as the Bitcoin

halving, which reduces the rate at which new Bitcoins are created. Transaction fees are paid by users to prioritize their transactions for inclusion in the next block.

Fees are dynamic and depend on network demand. During periods of high activity, fees can increase as users compete to have their transactions included in the next block. Conversely, when the network is less congested, fees tend to decrease. This fee market helps ensure that miners continue to secure the network even as block rewards diminish over time.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

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

2. Rent Fees:

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

3. Smart Contract Fees:

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

H.6 Use of distributed ledger technology

No, DLT not operated by the issuer, offeror, a person seeking admission to trading or a third-party acting on the issuer's their behalf.

H.7 DLT functionality description

Not applicable.

H.8 Audit

Since the question of "technology" is understood in a broad sense, the answer to the question of whether an examination of the "technology used" has been carried out is "no, we cannot guarantee that all parts of the technology used have been examined." This is because this report focuses on risks and we cannot guarantee that every part of the technology used has been examined.

H.9 Audit outcome

Not applicable.

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

This white paper (drawn up from 2025-08-16) has been prepared with utmost caution; however, uncertainties in the regulatory requirements and future changes in regulatory frameworks could potentially impact the token's legal status and its tradability. There is also a high probability that other laws will come into force, changing the rules for the trading of the token. Therefore, such developments shall be monitored and acted upon accordingly.

2. Operational and Technical

Blockchain Dependency: The token is entirely dependent on the blockchain the crypto-asset is issued upon (as of 2025-08-16). Any issues, such as downtime, congestion, or security vulnerabilities within the blockchain, could adversely affect the token's functionality.

Smart Contract Risks: Smart contracts governing the token may contain hidden vulnerabilities or bugs that could disrupt the token offering or distribution processes.

Connection Dependency: As the trading of the token also involves other trading venues, technical risks such as downtime of the connection or faulty code are also possible.

Human errors: Due to the irrevocability of blockchain-transactions, approving wrong transactions or using incorrect networks/addresses will most likely result in funds not being accessibly anymore.

Custodial risk: When admitting the token to trading, the risk of losing clients assets due to hacks or other malicious acts is given. This is due to the fact the token is hold in custodial wallets for the customers.

3. Market and Liquidity

Volatility: The token will most likely be subject to high volatility and market speculation. Price fluctuations could be significant, posing a risk of substantial losses to holders.

Liquidity Risk: Liquidity is contingent upon trading activity levels on decentralized exchanges (DEXs) and potentially on centralized exchanges (CEXs), should they be involved. Low trading volumes may restrict the buying and selling capabilities of the tokens.

4. Counterparty

As the admission to trading involves the connection to other trading venues, counterparty risks arise. These include, but are not limited to, the following risks:

General Trading Platform Risk: The risk of trading platforms not operating to the highest standards is given. Examples like FTX show that especially in nascent industries, compliance and oversight-frameworks might not be fully established and/or enforced.

Listing or Delisting Risks: The listing or delisting of the token is subject to the trading partners internal processes. Delisting of the token at the connected trading partners could harm or completely halt the ability to trade the token.

5. Liquidity

Liquidity of the token can vary, especially when trading activity is limited. This could result in high slippage when trading a token.

6. Failure of one or more Counterparties

Another risk stems from the internal operational processes of the counterparties used. As there is no specific oversight other than the typical due diligence check, it cannot be guaranteed that all counterparties adhere to the best market standards.

Bankruptcy Risk: Counterparties could go bankrupt, possibly resulting in a total loss for the clients assets hold at that counterparty.

7. Information asymmetry

Different groups of participants may not have the same access to technical details or governance information, leading to uneven decision-making and potential disadvantages for less informed investors.

I.2 Issuer-related risks

1. Insolvency

As with every other commercial endeavor, the risk of insolvency of the issuer is given. This could be caused by but is not limited to lack of interest from the public, lack of funding, incapacitation of key developers and project members, force majeure (including pandemics and wars) or lack of commercial success or prospects.

2. Counterparty

In order to operate, the issuer has most likely engaged in different business relationships with one or more third parties on which it strongly depends on. Loss or changes in the leadership or key partners of the issuer and/or the respective counterparties can lead to disruptions, loss of trust, or project failure. This could result in a total loss of economic value for the crypto-asset holders.

3. Legal and Regulatory Compliance

Cryptocurrencies and blockchain-based technologies are subject to evolving regulatory landscapes worldwide. Regulations vary across jurisdictions and may be subject to significant changes. Non-compliance can result in investigations, enforcement actions, penalties, fines, sanctions, or the prohibition of the trading of the crypto-asset impacting its viability and market acceptance. This could also result in the issuer to be subject to

private litigation. The beforementioned would most likely also lead to changes with respect to trading of the crypto-asset that may negatively impact the value, legality, or functionality of the crypto-asset.

4. Operational

Failure to develop or maintain effective internal control, or any difficulties encountered in the implementation of such controls, or their improvement could harm the issuer's business, causing disruptions, financial losses, or reputational damage.

5. Industry

The issuer is and will be subject to all of the risks and uncertainties associated with a crypto-project, where the token issued has zero intrinsic value. History has shown that most of this projects resulted in financial losses for the investors and were only set-up to enrich a few insiders with the money from retail investors.

6. Reputational

The issuer faces the risk of negative publicity, whether due to, without limitation, operational failures, security breaches, or association with illicit activities, which can damage the issuer reputation and, by extension, the value and acceptance of the crypto-asset.

7. Competition

There are numerous other crypto-asset projects in the same realm, which could have an effect on the crypto-asset in question.

8. Unanticipated Risk

In addition to the risks included in this section, there might be other risks that cannot be foreseen. Additional risks may also materialize as unanticipated variations or combinations of the risks discussed.

I.3 Crypto-assets-related risks

1. Valuation

As the crypto-asset does not have any intrinsic value, and grants neither rights nor obligations, the only mechanism to determine the price is supply and demand. Historically, most crypto-assets have dramatically lost value and were not a beneficial investment for the investors. Therefore, investing in these crypto-assets poses a high risk, and the loss of funds can occur.

2. Market Volatility

Crypto-asset prices are highly susceptible to dramatic fluctuations influence by various factors, including market sentiment, regulatory changes, technological advancements, and macroeconomic conditions. These fluctuations can result in significant financial losses within short periods, making the market highly unpredictable and challenging for investors. This is especially true for crypto-assets without any intrinsic value, and investors should be prepared to lose the complete amount of money invested in the respective crypto-assets.

3. Liquidity Challenges

Some crypto-assets suffer from limited liquidity, which can present difficulties when executing large trades without significantly impacting market prices. This lack of liquidity can lead to substantial financial losses, particularly during periods of rapid market movements, when selling assets may become challenging or require accepting unfavorable prices.

4. Asset Security

Crypto-assets face unique security threats, including the risk of theft from exchanges or digital wallets, loss of private keys, and potential failures of custodial services. Since crypto transactions are generally irreversible, a security breach or mismanagement can result in the permanent loss of assets, emphasizing the importance of strong security measures and practices.

5. Scams

The irrevocability of transactions executed using blockchain infrastructure, as well as the pseudonymous nature of blockchain ecosystems, attracts scammers. Therefore,

investors in crypto-assets must proceed with a high degree of caution when investing in if they invest in crypto-assets. Typical scams include – but are not limited to – the creation of fake crypto-assets with the same name, phishing on social networks or by email, fake giveaways/airdrops, identity theft, among others.

6. Blockchain Dependency

Any issues with the blockchain used, such as network downtime, congestion, or security vulnerabilities, could disrupt the transfer, trading, or functionality of the crypto-asset.

7. Smart Contract Vulnerabilities

The smart contract used to issue the crypto-asset could include bugs, coding errors, or vulnerabilities which could be exploited by malicious actors, potentially leading to asset loss, unauthorized data access, or unintended operational consequences.

8. Privacy Concerns

All transactions on the blockchain are permanently recorded and publicly accessible, which can potentially expose user activities. Although addresses are pseudonoymous, the transparent and immutable nature of blockchain allows for advanced forensic analysis and intelligence gathering. This level of transparency can make it possible to link blockchain addresses to real-world identities over time, compromising user privacy.

9. Regulatory Uncertainty

The regulatory environment surrounding crypto-assets is constantly evolving, which can directly impact their usage, valuation, and legal status. Changes in regulatory frameworks may introduce new requirements related to consumer protection, taxation, and anti-money laundering compliance, creating uncertainty and potential challenges for investors and businesses operating in the crypto space. Although the crypto-asset do not create or confer any contractual or other obligations on any party, certain regulators may nevertheless qualify the crypto-asset as a security or other financial instrument under their applicable law, which in turn would have drastic consequences for the crypto-asset, including the potential loss of the invested capital in the asset. Furthermore, this could lead to the sellers and its affiliates, directors, and officers being

obliged to pay fines, including federal civil and criminal penalties, or make the crypto-asset illegal or impossible to use, buy, or sell in certain jurisdictions. On top of that, regulators could take action against the issuer as well as the trading platforms if the the regulators view the token as an unregistered offering of securities or the operations otherwise as a violation of existing law. Any of these outcomes would negatively affect the value and/or functionality of the crypot-asset and/or could cause a complete loss of funds of the invested money in the crypto-asset for the investor.

10. Counterparty risk

Engaging in agreements or storing crypto-assets on exchanges introduces counterparty risks, including the failure of the other party to fulfill their obligations. Investors may face potential losses due to factors such as insolvency, regulatory non-compliance, or fraudulent activities by counterparties, highlighting the need for careful due diligence when engaging with third parties.

11. Reputational concerns

Crypto-assets are often subject to reputational risks stemming from associations with illegal activities, high-profile security breaches, and technological failures. Such incidents can undermine trust in the broader ecosystem, negatively affecting investor confidence and market value, thereby hindering widespread adoption and acceptance.

12. Technological Innovation

New technologies or platforms could render the network's design less competitive or even break fundamental parts (i.e., quantum computing might break cryptographic algorithms used to secure the network), impacting adoption and value. Participants should approach the crypto-asset with a clear understanding of its speculative and volatile nature and be prepared to accept these risks and bear potential losses, which could include the complete loss of the asset's value.

13. Community and Narrative

As the crypto-asset has no intrinsic value, all trading activity is based on the intended market value is heavily dependent on its community.

14. Interest Rate Change

Historically, changes in interest, foreign exchange rates, and increases in volatility have increased credit and market risks and may also affect the value of the crypto-asset. Although historic data does not predict the future, potential investors should be aware that general movements in local and other factors may affect the market, and this could also affect market sentiment and, therefore most likely also the price of the crypto-asset.

15. Taxation

The taxation regime that applies to the trading of the crypto-asset by individual holders or legal entities will depend on the holder's jurisdiction. It is the holder's sole responsibility to comply with all applicable tax laws, including, but not limited to, the reporting and payment of income tax, wealth tax, or similar taxes arising in connection with the appreciation and depreciation of the crypto-asset.

16. Anti-Money Laundering/Counter-Terrorism Financing

It cannot be ruled out that crypto-asset wallet addresses interacting with the crypto-asset have been, or will be used for money laundering or terrorist financing purposes, or are identified with a person known to have committed such offenses.

17. Market Abuse

It is noteworthy that crypto-assets are potentially prone to increased market abuse risks, as the underlying infrastructure could be used to exploit arbitrage opportunities through schemes such as front-running, spoofing, pump-and-dump, and fraud across different systems, platforms, or geographic locations. This is especially true for crypto-assets with a low market capitalization and few trading venues, and potential investors should be aware that this could lead to a total loss of the funds invested in the crypto-asset.

18. Timeline and Milestones

Critical project milestones could be delayed by technical, operational, or market challenges.

19. Legal ownership: Depending on jurisdiction, token holders may not have enforceable legal rights over their holdings, limiting avenues for recourse in disputes or cases of fraud.

20. Jurisdictional blocking: Access to exchanges, wallets, or interfaces may be restricted based on user location or regulatory measures, even if the token remains transferable on-chain.

21. Token concentration: A large proportion of tokens held by a few actors could allow price manipulation, governance dominance, or sudden sell-offs impacting market stability.

22. Ecosystem incentive misalignment: If validator, developer, or user rewards become unattractive or distorted, network security and participation could decline.

23. Governance deadlock: Poorly structured or fragmented governance processes may prevent timely decisions, creating delays or strategic paralysis.

24. Compliance misalignment: Features or delivery mechanisms may unintentionally conflict with evolving regulations, particularly regarding consumer protection or data privacy.

I.4 Project implementation-related risks

As this white paper relates to the "Admission to trading" of the crypto-asset, the implementation risk is referring to the risks on the Crypto Asset Service Providers side. These can be, but are not limited to, typical project management risks, such as key-personal-risks, timeline-risks, and technical implementation-risks.

I.5 Technology-related risks

As this white paper relates to the "Admission to trading" of the crypto-asset, the technology-related risks mainly involve the DLT networks where the crypto asset is issued in.

1. Blockchain Dependency Risks

Network Downtime: Potential outages or congestion on the involved blockchains could interrupt on-chain token transfers, trading, and other functions.

2. Smart Contract Risks

Vulnerabilities: The smart contract governing the token could contain bugs or vulnerabilities that may be exploited, affecting token distribution or vesting schedules.

3. Wallet and Storage Risks

Private Key Management: Token holders must securely manage their private keys and recovery phrases to prevent permanent loss of access to their tokens, which includes Trading-Venues, who are a prominent target for dedicated hacks.

Compatibility Issues: The tokens require compatible wallets for storage and transfer. Any incompatibility or technical issues with these wallets could impact token accessibility.

4. Network Security Risks

Attack Risks: The blockchains may face threats such as denial-of-service (DoS) attacks or exploits targeting its consensus mechanism, which could compromise network integrity.

Centralization Concerns: Although claiming to be decentralized, the relatively smaller number of validators/concentration of stakes within the networks compared to other blockchains might pose centralization risks, potentially affecting network resilience.

5. Evolving Technology Risks: Technological Obsolescence: The fast pace of innovation in blockchain technology may make the used token standard appear less competitive or become outdated, potentially impacting the usability or adoption of the token.

6. Bridges: The dependency on multiple ecosystems can negatively impact investors. This asset bridge creates corresponding risks for investors, as this lock-in mechanism may not function properly for technical reasons or may be subject to attack. In that case, the supply may change immediately or the ownership rights to tokens may be changed.

7. Forking risk: Network upgrades may split the blockchain into separate versions, potentially creating duplicate tokens or incompatibility between different versions of the protocol.

8. Economic abstraction: Mechanisms such as gas relayers or wrapped tokens may allow users to bypass the native asset, reducing its direct demand and weakening its economic role.

9. Dust and spam attacks: Low-value transactions may flood the network, increasing ledger size, reducing efficiency, and exposing user addresses to tracking.

10. Frontend dependency: If users rely on centralised web interfaces or wallets, service outages or compromises could block access even if the blockchain itself continues to operate.

11. Risk of Runes

The use of "Runes technology" introduces a specific risk factor, as it represents a comparatively novel and untested technical standard within the crypto-asset environment. Given the limited operational history and the absence of long-term empirical evidence, the resilience and reliability of this implementation under stressed market conditions cannot be assured.

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

39120077M9TG0O1FE250

S.3 Name of the cryptoasset

MAGIC INTERNET MONEY

S.4 Consensus Mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana and Bitcoin (via so called "Runes"). In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Bitcoin/Runes:

The consensus mechanism from Bitcoin is Proof-of-Work (PoW), which intends to provide security and decentralization. In PoW, miners calculate a hash function of their respective newly proposed blocks, a summary of the previous block and a nonce variable. The nonce variable is adjusted until the result of the hash function satisfies a predefined difficulty target. In a computational sense it is very difficult to find a suitable nonce, but it is very easy to verify it. When a miner finds a suitable nonce, the new block including the nonce is broadcast to other nodes to be verified. Verified blocks are then added to the blockchain. The miner who made the block is rewarded. Every 2016 blocks (around 2 Weeks) the network automatically adjusts the difficulty target, to maintain a block time of around 10 minutes. The network follows the longest chain rule, where nodes always consider the longest valid chain as the correct version.

The following applies to Solana:

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

Core Concepts

1. Proof of History (PoH):

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

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

2. Proof of Stake (PoS):

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

selected to validate transactions and produce new blocks.

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

cryptographic clock for the network.

3. Block Production:

The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator

uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order.

4. Consensus and Finalization:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

S.5 Incentive Mechanisms and Applicable Fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana and Bitcoin (via so called "Runes"). In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Bitcoin/Runes:

The incentive mechanism of Bitcoin is designed to encourage miners to secure the network and validate transactions. Miners are rewarded with block rewards (newly minted Bitcoins) and transaction fees for every block that they add to the chain. The block reward is halved approximately every four years in an event known as the Bitcoin halving, which reduces the rate at which new Bitcoins are created. Transaction fees are paid by users to prioritize their transactions for inclusion in the next block.

Fees are dynamic and depend on network demand. During periods of high activity, fees can increase as users compete to have their transactions included in the next block. Conversely, when the network is less congested, fees tend to decrease. This fee market helps ensure that miners continue to secure the network even as block rewards diminish over time.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

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

2. Rent Fees:

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

3. Smart Contract Fees:

Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This is

intended to ensure that users are charged proportionally for the resources they consume.

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

2024-08-25

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

2025-08-25

S.8 Energy consumption

54297860.16846 kWh/a

S.9 Energy consumption sources and methodologies

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

S.10 Renewable energy consumption

29.3064258533 %

S.11 Energy intensity

0.49161 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

22370.50361 tCO2e/a

S.14 GHG intensity

0.20254 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.