CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

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

Preamble

00. Table of Contents

01. Date of notification

This white paper was notified on 2026-06-30.

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 OFFICIAL TRUMP crypto-asset referred to in this white paper is a crypto-asset other than an EMT or ART. It is natively implemented on the Solana blockchain and is also available on the TRON blockchain, according to the DTI FFG shown in section F.14, as of 2026-06-22. The maximum supply of TRUMP is set at 1,000,000,000 tokens, scheduled for release over three years.

The initial production of the tokens, the so-called “mint”, took place on 2025-01-17 at 14:01:48 UTC (signature: UFec7orzRrt17gDr6NpB1dNGwoKBSHyyEww94KJcZa4gFNYTBH2yWPVZDB4L5Gp4jsrPs9efwxWGdqGai4XKWtG, source: https://solscan.io/tx/UFec7orzRrt17gDr6NpB1dNGwoKBSHyyEww94KJcZa4gFNYTBH2yWPVZDB4L5Gp4jsrPs9efwxWGdqGai4XKWtG, accessed 2026-06-22). The first activity on TRON can be viewed on 2025-07-23 (transaction hash: 46506c8ebd74153d0b1ee78dfd8efcfdc0458914d3b50251f443a1ddd4b3141f, source: https://tronscan.org/transaction/46506c8ebd74153d0b1ee78dfd8efcfdc0458914d3b50251f443a1ddd4b3141f/overview, accessed 2026-06-22).

As outlined on the project’s website (https://gettrumpmemes.com/, accessed 2026-06-22), 200,000,000 tokens were fully unlocked at the date of the initial mint on 2025-01-17. The remaining 800,000,000 tokens were set to be gradually released over the 36 months following the date of the initial mint. According to statements made on the aforementioned website, CIC Digital LLC, an affiliate of The Trump Organization, and Fight Fight Fight LLC collectively own 80% of the TRUMP token supply, subject to a three-year unlocking schedule. The website also states that these tokens are subject to lock-up periods ranging from 3 to 12 months and are subsequently unlocked linearly over a 24-month period. The remaining tokens are stated to be allocated as 10% reserved for liquidity and 10% for public distribution, both of which were fully unlocked at launch.

According to publicly available information (source: https://gettrumpmemes.com/, accessed 2026-06-22), TRUMP is a meme crypto-asset made available through GetTrumpMemes.com and presented as the official Trump meme. The holding of TRUMP is associated with the $TRUMP Coin Club, a tiered membership programme through which holders may be offered leaderboard-based rewards, merchandise discounts and access to events. Material information relating to the crypto-asset is published by Fight Fight Fight LLC through its recognised disclosure channels, principally the project website.

According to the issuer's terms and conditions (source: https://gettrumpmemes.com/terms, accessed 2026-06-22), TRUMP is intended to function as an expression of support for and engagement with the ideals and beliefs embodied by the symbol "$TRUMP" and the associated artwork, and is expressly stated not to be an investment opportunity, investment contract or security of any type.

According to the $TRUMP Coin Club page (source: https://gettrumpmemes.com/trumpclub, accessed 2026-06-22), the crypto-asset has no payment functionality and is not redeemable for goods, services or cash, in the sense that the tokens are not surrendered or exchanged in return for any benefit. Holders may nonetheless, on the basis of their time-weighted holdings and at the issuer's sole discretion, be offered access to events, experiences and merchant discounts through the $TRUMP Coin Club. According to the same source, neither the holding of TRUMP nor the amount held entitles, guarantees or confers any right or claim to any specific benefit, reward, service or experience.

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

Fight Fight Fight LLC

B.3 Legal form

The legal form of Fight Fight Fight LLC is HZEH, which corresponds to "Limited Liability Company".

B.4 Registered address

The registered address of Fight Fight Fight LLC is 251 Little Falls Drive, Wilmington, DE 19808,

United States,

US-DE

B.5 Head office

The head office address of Fight Fight Fight LLC is 516 S. Dixie Highway, Suite 195, West Palm Beach, FL 33401,

United States,

US-FL

B.6 Registration date

Fight Fight Fight LLC was registered on 2025-01-07.

B.7 Legal entity identifier

A legal identifier was not available at the time of writing this white paper (2026-06-22).

B.8 Another identifier required pursuant to applicable national law

Delaware File Number: 10052401

B.9 Parent company

Due to the unavailability of certain corporate documents, the parent company or parent companies of Fight Fight Fight LLC could not be determined with certainty at the time of writing this white paper (2026-06-22). The project website states that Celebration Cards LLC is the owner of Fight Fight Fight LLC, while CIC Digital LLC, an affiliate of The Trump Organization, and Fight Fight Fight LLC are stated to collectively own 80% of the TRUMP token supply. However, the full ownership and control structure could not be independently verified from official corporate records. CIC Digital LLC was incorporated on 2022-03-01 and is registered under file number 6646611, with its registered address at 251 Little Falls Drive, Wilmington, DE 19808, United States, and telephone number +1 302 636 5401. Celebration Cards LLC was incorporated on 1999-06-23 and is registered in the State of New York under entity ID 2391597.

B.10 Members of the management body

Identity	Function	Business Address
Could not be identified	Not applicable	Not applicable

B.11 Business activity

Based on the project website and the associated terms and conditions, Fight Fight Fight LLC operates, or is associated with the operation of, GetTrumpMemes.com and the related TRUMP services, including the TRUMP Coin Club membership programme and the publication of material token-related disclosures through its designated disclosure channels. No broader registered business activity of Fight Fight Fight LLC could be identified from publicly available corporate records (sources accessed 2026-06-22).

B.12 Parent company business activity

Due to publicly unavailable corporate documents, the business activity of the parent company/ companies of Fight Fight Fight LLC could not be identified.

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

C.1 Name

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

C.2 Legal form

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

C.3 Registered address

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

C.4 Head office

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

C.5 Registration date

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

C.6 Legal entity identifier

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

C.7 Another identifier required pursuant to applicable national law

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

C.8 Parent company

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

C.9 Reason for crypto-asset white paper preparation

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

C.10 Members of the management body

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

C.11 Operator business activity

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

C.12 Parent company business activity

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

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

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

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

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

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "OFFICIAL TRUMP", Short Name: "TRUMP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-06-22).

D.2 Crypto-assets name

Long Name: "OFFICIAL TRUMP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-06-22).

D.3 Abbreviation

Short Name: "TRUMP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F. 13, FFG DTI see F.14 as of 2026-06-22).

D.4 Crypto-asset project description

According to publicly available information (sources: https://gettrumpmemes.com/ and https://gettrumpmemes.com/trumpclub, accessed 2026-06-22), OFFICIAL TRUMP is a meme crypto-asset project operated by Fight Fight Fight LLC through the website GetTrumpMemes.com and presented as the only official Trump meme. The stated purpose of the project is to function as an expression of support for, and engagement with, the ideals and beliefs associated with the symbol "$TRUMP" and the related artwork, and to build a community around that brand.

The principal component of the project is the $TRUMP Coin Club, a tiered membership programme (source: https://gettrumpmemes.com/trumpclub, accessed 2026-06-22). On the basis of time-weighted holdings, members may be offered leaderboard-based rewards, discounts across merchandise lines such as TRUMP Watches, TRUMP Sneakers and TRUMP Fragrances and other merchant partners, commemorative items, and access to events and experiences. Events offered under or alongside the project have included a private gala dinner for top holders held on 2025-05-22 and a "Crypto & Business Conference" at Mar-a-Lago on 2026-04-25, with further experiences announced during 2026. The availability and scope of any such benefit are stated to be at the issuer's sole discretion and may be modified or cancelled.

The project is operated by Fight Fight Fight LLC. Together with CIC Digital LLC, an affiliate of The Trump Organization, Fight Fight Fight LLC holds 80% of the supply subject to a three-year unlocking schedule, and CIC Digital LLC and Celebration Cards LLC (the owner of Fight Fight Fight LLC) are stated to receive trading revenue derived from trading activity. The "TRUMP" trademark is owned by DTTM Operations LLC and used under licence. Within the project the crypto-asset serves as the means of engagement and of access to the Coin Club, and does not represent any ownership, equity, profit-participation, governance or redemption right. The functionality and legal characteristics of the crypto-asset, including the absence of any enforceable right to Coin Club benefits, are described in section F.2.

The long-term evolution of the project, including the scope of any Coin Club benefits, merchant partnerships and events, may vary based on commercial, technical, economic and regulatory considerations. All future developments remain subject to change.

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

Name of person	Type of person	Business address of person	Domicile of company
Fight Fight Fight LLC	Other person involved in implementation	516 S. Dixie Highway, Suite 195, West Palm Beach, FL 33401, United States	United States
CIC Digital LLC	Other person involved in implementation	Corporation Service Company, 251 Little Falls Drive, Wilmington, New Castle, DE 19808, United States	United States
Celebration Cards LLC	Other person involved in implementation	29-16 Ditmars Blvd., Astoria, NY 11105, United States	United States
DTTM Operations LLC	Other person involved in implementation	Corporation Service Company, 251 Little Falls Drive, Wilmington, New Castle, DE 19808, United States	United States
Donald J. Trump	Other person involved in implementation	Palm Beach, FL, United States	United States

Name of person	Type of person	Business address of person	Domicile of company
Bill Zanker	Other person involved in implementation	c/o Fight Fight Fight LLC, 516 S. Dixie Highway, Suite 195, West Palm Beach, FL 33401, United States	United States

D.6 Utility Token Classification

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

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

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

D.8 Plans for the token

This section provides an overview of the historical developments related to the TRUMP crypto-asset and a description of planned or anticipated project milestones as publicly communicated. All forward-looking elements are subject to significant uncertainty. They do not constitute commitments, assurances or guarantees, and may be modified, delayed or discontinued at any time.

There is no single formally published roadmap for the TRUMP token; project plans are communicated through the project website and public announcements (sources: https://gettrumpmemes.com/, https://gettrumpmemes.com/trumpclub, https://gettrumpmemes.com/market-update and https://gettrumpmemes.com/trump-coin-grants, accessed 2026-06-22).

Past milestones:

- Brand origin (2024-07-13): the project identifies the "Fight Fight Fight" moment of 2024-07-13 as the genesis of the meme on which the crypto-asset is based (source: https://gettrumpmemes.com/, accessed 2026-06-22).

- Token launch on Solana (2025-01-17): the full supply of 1,000,000,000 TRUMP was created in a single mint transaction, of which 200,000,000 (20%) were unlocked at launch.

- Top-holder dinner announced (2025-04-23): the issuer announced a contest, running to 2025-05-12, under which the top 220 holders would be invited to a gala dinner with President Trump, the top 25 to a VIP reception and the top holders to a TRUMP-branded watch.

- Gala dinner held (2025-05-22): the gala dinner for the top 220 holders took place at Trump National Golf Club, Washington DC.

- TRON deployment (2025-07-23): TRUMP was made available on the TRON network as a LayerZero Omnichain Fungible Token, that is, a bridged representation of the Solana asset.

- Market structure and ecosystem update (2026-02-22): the project announced a "next phase" comprising yield and liquidity programmes (Kamino vaults), institutional market makers, the deployment of less than 5% of supply for ecosystem initiatives, the $TRUMP Fund (up to USD 3,500,000) and a $TRUMP Game Studio (source: https://gettrumpmemes.com/market-update, accessed 2026-06-22).

- Crypto & Business Conference at Mar-a-Lago (2026-04-25): a conference featuring President Trump, at which the America First Business Challenge was debuted (sources: https://gettrumpmemes.com/trumpclub and https://gettrumpmemes.com/trump-coin-grants, accessed 2026-06-22; US Senate letter dated 2026-04-08).

- Summer 2026 Coin Club leaderboard opened (2026-05-08): a holdings-based leaderboard, running to 2026-07-01, determining tiered $TRUMP Coin Club membership rewards.

- America First Business Challenge launched (2026-05-14): a 90-day entrepreneurship competition awarding up to USD 1,000,000 in $TRUMP grants, funded by the $TRUMP platform (source: https://gettrumpmemes.com/trump-coin-grants, accessed 2026-06-22).

Future Milestones:

- $TRUMP Coin Club top-tier rewards (2026-07-19): a private suite at the FIFA World Cup 2026 final and a watch party at Trump Tower, New York, for top-ranked holders (source: https://gettrumpmemes.com/trumpclub, accessed 2026-06-22).

- America First Business Challenge live finale (July 2026), at which finalists pitch before the judging panel (source: https://gettrumpmemes.com/trump-coin-grants, accessed 2026-06-22).

- Yield and liquidity programmes: holder participation in Kamino vaults supported by more than USD 10,000,000 in $TRUMP incentives, alongside continued institutional market-making (source: https://gettrumpmemes.com/market-update, accessed 2026-06-22).

- Ecosystem investment: the $TRUMP Fund (up to USD 3,500,000, with grants of USD 50,000 to USD 250,000) and the $TRUMP Game Studio, beginning with the TRUMP Billionaires Club game (source: https://gettrumpmemes.com/market-update, accessed 2026-06-22).

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments and market adoption. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes

do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the TRUMP crypto-asset for its holders.

D.9 Resource allocation

Based on publicly available information, the TRUMP project was not financed through disclosed equity investment or venture capital rounds, and no pre-sale to identified investors has been identified. At launch on 2025-01-17, the full supply of 1,000,000,000 TRUMP tokens was minted, with 200,000,000 tokens made available at launch and the remaining 800,000,000 tokens subject to release over a three-year period. The resources associated with the project are therefore understood to derive primarily from the initial token distribution, retained token holdings and trading-related revenue, rather than from external financing.

According to the project website, the 200,000,000 tokens made available at launch consisted of 100,000,000 tokens reserved for liquidity and 100,000,000 tokens allocated for public distribution. The remaining 800,000,000 tokens are held by entities associated with the project and are subject to the above-mentioned three-year unlocking schedule. The project website further states that entities associated with the project receive trading revenue derived from trading activity in the token.

Public reporting has published different estimates of monetary amounts associated with the TRUMP token. A Financial Times analysis published in March 2025 reported that wallets attributed to entities operating the project received at least USD 350,000,000 during the initial weeks after launch, consisting of approximately USD 314,000,000 from token sales and approximately USD 36,000,000 from liquidity-pool fees. Separately, Reuters reported on 2025-02-03, citing third-party blockchain analysis estimates, that entities behind the token had accumulated trading fees of between USD 86,000,000 and USD 100,000,000 by 2025-01-30. These figures relate to different methodologies, measurement windows and categories of value, and should not be aggregated.

Public reporting has also referred to the notional market value of retained or locked token holdings. Such figures are price-dependent and may fluctuate materially with market conditions. They should not be read as realised proceeds, cash resources or verified project funding.

According to the project's market-structure update of 2026-02-22, less than 5% of the TRUMP token supply is expected to be deployed, sold, distributed or otherwise monetised over the following months to fund ecosystem initiatives. The exact amount of proceeds realised from token sales, trading-related revenue and future monetisation of retained tokens cannot be independently verified from publicly available information.

Accordingly, no single reliable aggregate amount of financial resources allocated to the project can be stated on the basis of the available public information. The principal identifiable resources consist of retained TRUMP token holdings, proceeds reportedly generated through token sales and trading-related revenue. On-chain data may be used to observe token balances and transfers on Solana; however, a public blockchain address cannot necessarily be attributed to a single natural or legal person. This limits the ability to determine exact economic control, beneficial ownership, realised proceeds or future actions. Changes in token distribution, unlocks, sales or monetisation of retained tokens may negatively affect holders of the TRUMP token.

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

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

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

E.1 Public offering or admission to trading

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

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The maximum supply of the crypto-asset is set at 1,000,000,000 units. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning". As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

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

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

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

E.35 Trading platforms access

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

E.36 Involved costs

The costs involved in accessing the trading platform depend on the specific fee structure and terms of the respective crypto-asset service provider. These may include trading fees, deposit or withdrawal charges, and network-related 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 crypto-asset does not aim to maintain a stable value by referencing an official currency, a basket of assets, or any other underlying rights. Instead, its valuation is entirely market-driven, based on supply and demand dynamics, and it is not subject to any stabilisation mechanism. It is neither pegged to any fiat currency nor backed by any external assets, which distinguishes it from EMTs and ARTs. Furthermore, the crypto-asset is not categorised as a financial instrument, deposit, insurance product, pension product, or any other regulated financial product under EU law. It does not grant financial rights, voting rights, or any contractual claims to its holders, and therefore remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

TRUMP is a fungible crypto-asset implemented natively on the Solana network as an SPL token and additionally available on the TRON network as a TRC-20 token. The token is intended to function as an expression of support for, and engagement with, the ideals and beliefs embodied by the symbol "$TRUMP" and the associated artwork. It has no inherent technical or economic function beyond being held and transferred.

The only holding-related feature identified is the $TRUMP Coin Club (source: https://gettrumpmemes.com/trumpclub, accessed 2026-06-22). On the basis of time-weighted holdings and at the issuer's sole discretion, holders may be offered access to events, experiences and merchant discounts. This is an off-chain promotional arrangement operated by the issuer, not a function of the token itself, and according to the same source neither the holding of TRUMP nor the amount held entitles, guarantees or confers any right or claim to any specific benefit, reward, service or experience.

Beyond the above, TRUMP has no protocol-level functionality as of the date of this white paper. It has no payment functionality, no transactional utility and no commercial integration, and is not redeemable for goods, services or cash. It does not entitle holders to any yield, fee share, dividend, redemption, staking reward or governance right.

The TRUMP token does not confer ownership, profit participation, governance rights over the issuer or any related entity in a corporate-law sense, or any form of legally enforceable economic entitlement. TRUMP is a standard fungible token with no protocol environment of its own, and its transfer and custody depend on factors such as the stability and operational conditions of the Solana and TRON blockchains, which are outside the control of token holders.

F.3 Planned application of functionalities

Future Milestones:

- $TRUMP Coin Club top-tier rewards (2026-07-19): a private suite at the FIFA World Cup 2026 final and a watch party at Trump Tower, New York, for top-ranked holders (source: https://gettrumpmemes.com/trumpclub, accessed 2026-06-22).

- America First Business Challenge live finale (July 2026), at which finalists pitch before the judging panel (source: https://gettrumpmemes.com/trump-coin-grants, accessed 2026-06-22).

- Yield and liquidity programmes: holder participation in Kamino vaults supported by more than USD 10,000,000 in $TRUMP incentives, alongside continued institutional market-making (source: https://gettrumpmemes.com/market-update, accessed 2026-06-22).

- Ecosystem investment: the $TRUMP Fund (up to USD 3,500,000, with grants of USD 50,000 to USD 250,000) and the $TRUMP Game Studio, beginning with the TRUMP Billionaires Club game (source: https://gettrumpmemes.com/market-update, accessed 2026-06-22).

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

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

The type of submission is MODI (Modified white paper).

F.6 Crypto-asset characteristics

The crypto-asset is a crypto-asset other than an e-money token or an asset-referenced token, and is available on the Solana and TRON blockchains. It is fungible, with divisibility to 6 decimal places on Solana and to 18 decimal places on TRON. A total of 1,000,000,000 units has been issued. The

crypto-asset constitutes a digital representation of value recorded using distributed-ledger technology and does not confer ownership, governance, profit-participation, or any other legally enforceable rights. Any functionalities associated with the crypto-asset are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The value of the crypto-asset, 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: "OFFICIAL TRUMP" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-06-22).

F.8 Website of the issuer

https://gettrumpmemes.com

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

2025-03-31

F.10 Publication date

2025-06-16

F.11 Any other services provided by the issuer

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

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

EN

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

13D4K4NW6; 3R313RR9C

F.14 Functionally fungible group digital token identifier

LJDPGNXXK

F.15 Voluntary data flag

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

F.16 Personal data flag

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

F.17 LEI eligibility

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

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on future public offers was not available at the time of writing this white paper (2026-06-22).

G.5 Issuer retained crypto-assets

According to the project's published disclosures, 800,000,000 TRUMP, equal to 80% of the maximum supply of 1,000,000,000 tokens, are retained by CIC Digital LLC, an affiliate of The Trump Organization, and Fight Fight Fight LLC (source: https://gettrumpmemes.com/, accessed 2026-06-22). These tokens are subject to a three-year unlocking schedule from the initial mint of

2025-01-17, with lock-up periods of 3 to 12 months followed by linear release over 24 months, expected to conclude on or about 2028-01-17.

The token distribution can be traced on-chain on Solana: https://solscan.io/token/6p6xgHyF7AeE6TZkSmFsko444wqoP15icUSqi2jfGiPN#holders. Public addresses cannot necessarily be assigned to a single person or entity. Changes in issuer-related holdings may negatively impact the investor.

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 implemented as of 2026-06-22. Furthermore, the supply cannot be increased because mint authority for the token was permanently forfeited. 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 implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

The following applies to Solana:

The crypto-asset is implemented on the Solana blockchain, a decentralised distributed-ledger network designed to support transaction processing and the execution of on-chain programs. The network relies on a set of technical protocols, cryptographic standards, and program frameworks intended to enable secure transaction validation, deterministic execution of instructions, and interoperability across the Solana ecosystem. The most relevant technical standards and protocols are outlined below.

1. Network Architecture and Core Protocols

The Solana network is structured as a peer-to-peer validator network in which independent nodes maintain the distributed ledger and process transactions.

- Solana uses Proof-of-History (PoH) as a cryptographic timing and ordering mechanism, while validator participation and voting are stake-weighted under its Proof-of-Stake model and Tower BFT consensus process.

- Tower BFT: A Byzantine fault tolerant consensus mechanism, derived from PBFT, that governs validator voting and block confirmation.

- Turbine: A block propagation protocol that distributes blocks across the validator network by splitting them into smaller data fragments ("shreds") and transmitting them through a layered tree-based structure.

- Gulf Stream: A transaction forwarding mechanism that routes transactions directly to upcoming block producers and thereby limiting the need for a global transaction mempool.

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

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

2. Address and Cryptographic Standards

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

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

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

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

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

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

3. Networking and Data Transmission Standards

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

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

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

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

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

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

4. Token and Program Standards (Solana Program Library)

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

Within this framework:

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

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

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

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

5. Protocol Development and Improvement Standards

Technical changes to the Solana protocol may be proposed and discussed through Solana Improvement Documents (SIMDs). These proposals document suggested modifications to protocol

behaviour, economic parameters, or technical limits. Accepted changes may be implemented through updates to validator software and related developer tooling used by network participants.

The following applies to TRON:

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 operates on the TRON blockchain, which is based on a decentralised, peer-to-peer networking architecture. Nodes communicate using a combination of gRPC and HTTP interfaces, with gRPC serving as the primary high-performance channel for block, transaction, and contract-execution communication.

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

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

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

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

2. Transaction and Address Standards

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

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

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

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

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

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

3. Blockchain Data Structure and Block Standards

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

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

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

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

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

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

4. Upgrade and Improvement Standards

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

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

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

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

H.3 Technology used

The crypto-asset in scope is implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

The following applies to Solana:

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

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

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

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

Security Protocols for Asset Custody and Transactions:

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

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

The following applies to TRON:

1. Private Key Management

TRON accounts are controlled through ECDSA key pairs (secp256k1). The private key is required for authorising all transactions and must be protected securely, as anyone with access can control the corresponding account. Users typically secure their keys through hardware wallets or other cold-

storage methods. TRON also supports advanced permission management, allowing accounts to assign multiple keys with weighted signatures across Owner, Active, and Witness permission groups.

2. Decentralized Ledger

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

3. Cryptographic Integrity and Hashing

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

4. TRC Standards for Fungible and Non-Fungible Assets

TRON supports multiple token standards.

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

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

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

H.4 Consensus mechanism

The crypto-asset in scope is implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

The following applies to Solana:

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

Core Concepts

1. Proof-of-History (PoH):

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

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

2. Proof-of-Stake (PoS):

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

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

3. Block Production:

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

4. Consensus and Finalisation:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

The following applies to TRON:

TRON uses a Delegated Proof of Stake (DPoS) consensus mechanism in which holders of the native crypto-asset may stake their units to obtain voting rights. These votes determine the 27 Super Representatives (SRs) that are responsible for block production. The SR set and block production order are updated during maintenance periods, which occur approximately every six hours. Blocks are produced in scheduled slots of approximately three seconds. If an SR does not produce a block in its assigned slot, the slot remains empty and the next scheduled SR may produce a block in the following slot.

Newly produced blocks are initially unconfirmed. A block is considered irreversible once it has been approved by more than 70% of the 27 SRs, meaning at least 19 SRs, through the production of subsequent blocks. Governance and adjustable protocol parameters are handled through an on-chain proposal system. Proposals may be initiated by SRs, SR partners and SR candidates, while only SRs may vote. A proposal is valid for three days and passes if it receives at least 18 SR votes.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

2. Rent Fees:

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

3. Program Execution Costs:

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

The following applies to TRON:

Super Representatives receive block production rewards for blocks they successfully produce. Current TRON documentation describes the block production reward as 8 units of the native crypto-asset per block, while an additional 128 units per block are allocated as voting rewards shared among SRs and SR partners based on votes received. SRs and SR partners may deduct a commission before distributing rewards to voters according to voting weight.

Transactions and smart-contract executions consume network resources. Standard transactions consume Bandwidth, while smart-contract deployment and execution also consume Energy. Users may obtain Bandwidth or Energy by staking the native crypto-asset. Where available resources are insufficient, the protocol burns the native crypto-asset to pay the applicable resource cost. The network also applies a dynamic Energy model, under which contracts that consume substantial resources during a maintenance cycle may require increased Energy in a subsequent cycle. TRON does not apply a conventional slashing mechanism, but failed or abnormal contract executions and the dynamic Energy model may result in higher resource deductions or costs.

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

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

H.9 Audit outcome

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

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Trading venue and connection risk

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

3. Market formation and liquidity conditions

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

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

4. Counterparty and service provider dependence

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

Quality of counterparties: Trading venues and service providers in certain jurisdictions may operate under regulatory or supervisory standards that are lower or differently enforced than those applicable in the European Union. In such environments, deficiencies in governance, risk

management, or compliance may remain undetected, which increases the probability of abrupt service interruptions, investigations, or forced wind-downs.

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

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

5. Operational and information risks

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

6. Market access and liquidity concentration risk

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

I.2 Issuer-related risks

1. Insolvency of the issuer

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

2. Legal and regulatory risks

The issuer operates in a dynamic and evolving regulatory environment. Failure to comply with applicable laws or regulations in relevant jurisdictions may result in enforcement actions, penalties,

or restrictions on the project's operations. These may negatively impact the crypto-asset's availability, market acceptance, or legal status.

3. Operational risks

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

4. Governance and decision-making

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

5. Reputational risks

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

6. Counterparty dependence

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

I.3 Crypto-assets-related risks

1. Valuation risk

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

2. Market volatility risk

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

3. Liquidity and price-determination risk

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

4. Crypto-asset security risk

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

5. Fraud and scam risk

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

6. Legal and regulatory reclassification risk

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

7. Absence of investor protection

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

8. Counterparty risk

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

9. Reputational risk

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

10. Community and sentiment risk

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

11. Macroeconomic and interest-rate risk

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

12. Taxation risk

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

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

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

14. Market-abuse risk

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

15. Legal ownership and jurisdictional risk

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

16. Concentration risk

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

I.4 Project implementation-related risks

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

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

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

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

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

I.5 Technology-related risks

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

1. Blockchain dependency risk

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

2. Smart contract vulnerability risk

The crypto-asset is implemented on more than one network, and the relevant technical risk differs by implementation. On the Solana network, the crypto-asset relies on shared token-program

infrastructure rather than a project-specific smart contract governing its transfers; the parameters of the associated mint account, including the status and configuration of the mint authority, are therefore the principal factor for supply-related and transfer-related risk on that network. On the TRON network, the crypto-asset is represented through a TRC-20-compatible LayerZero Omnichain Fungible Token (OFT) contract. Coding errors, misconfiguration or security vulnerabilities in that contract, in its trusted peers, in the cross-chain messaging configuration or in related interoperability infrastructure may result in failed or incorrectly credited transfers, loss of assets, duplication, or disruption of cross-chain functionality. On either network, undetected vulnerabilities may persist even after external audits, owing to the immutable nature of deployed code.

3. Wallet and key-management risk

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

Outdated or vulnerable wallet software:

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

4. Network security risks

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

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

5. Bridge and interoperability risk

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

6. Forking and protocol-upgrade risk

Network upgrades or disagreements among node operators or validators can result in blockchain “forks”, where the blockchain splits into two or more incompatible versions that continue separately

from a shared past. This may lead to duplicate token representations or incompatibilities between exchanges and wallets. Until consensus stabilises, trading or transfers may be disrupted or misaligned. Such situations may be difficult for retail holders to navigate, particularly when trading platforms or wallets display inconsistent token information.

7. Economic-layer and abstraction risk

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

8. Spam and network-efficiency risk

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

9. Front-end and access-interface risk

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

10. Decentralisation claim risk

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the crypto-asset

OFFICIAL TRUMP

S.4 Consensus Mechanism

The crypto-asset in scope is implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

The following applies to Solana:

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

Core Concepts

1. Proof-of-History (PoH):

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

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

2. Proof-of-Stake (PoS):

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

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

3. Block Production:

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

4. Consensus and Finalisation:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

The following applies to TRON:

TRON uses a Delegated Proof of Stake (DPoS) consensus mechanism in which holders of the native crypto-asset may stake their units to obtain voting rights. These votes determine the 27 Super Representatives (SRs) that are responsible for block production. The SR set and block production order are updated during maintenance periods, which occur approximately every six hours. Blocks are produced in scheduled slots of approximately three seconds. If an SR does not produce a block in its assigned slot, the slot remains empty and the next scheduled SR may produce a block in the following slot.

Newly produced blocks are initially unconfirmed. A block is considered irreversible once it has been approved by more than 70% of the 27 SRs, meaning at least 19 SRs, through the production of subsequent blocks. Governance and adjustable protocol parameters are handled through an on-chain proposal system. Proposals may be initiated by SRs, SR partners and SR candidates, while only SRs may vote. A proposal is valid for three days and passes if it receives at least 18 SR votes.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is implemented on the Solana network and is also available on the TRON blockchain, following the standards described below.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

Solana staking documentation notes slashing as a possible future mechanism for intentional malicious conduct, but states that slashing is not implemented in the protocol today. Economic

alignment instead currently arises primarily from staking participation, validator performance incentives, and the opportunity cost of locking capital in staking positions.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

2. Rent Fees:

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

3. Program Execution Costs:

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

The following applies to TRON:

Super Representatives receive block production rewards for blocks they successfully produce. Current TRON documentation describes the block production reward as 8 units of the native crypto-asset per block, while an additional 128 units per block are allocated as voting rewards shared among SRs and SR partners based on votes received. SRs and SR partners may deduct a commission before distributing rewards to voters according to voting weight.

Transactions and smart-contract executions consume network resources. Standard transactions consume Bandwidth, while smart-contract deployment and execution also consume Energy. Users may obtain Bandwidth or Energy by staking the native crypto-asset. Where available resources are insufficient, the protocol burns the native crypto-asset to pay the applicable resource cost. The network also applies a dynamic Energy model, under which contracts that consume substantial resources during a maintenance cycle may require increased Energy in a subsequent cycle. TRON does not apply a conventional slashing mechanism, but failed or abnormal contract executions and the dynamic Energy model may result in higher resource deductions or costs.

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

2025-06-29

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

2026-06-29

S.8 Energy consumption

2112.83580 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 network Solana and TRON 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

27.0081797971 %

S.11 Energy intensity

0.00000 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.73761 tCO2e/a

S.14 GHG intensity

0.00000 kgCO2e

S.15 Key energy sources and methodologies

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

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

Electricity Data"; Energy Institute, "Statistical Review of World Energy". Retrieved from: https://ourworldindata.org/grapher/share-electricity-renewables

S.16 Key GHG sources and methodologies

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

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.