CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG 3XVWCVFSX

Preamble

00. Table of Contents

01. Date of notification

2025-10-06

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

Since the token has multiple functions (hybrid token), these are already conceptually not utility tokens within the meaning of the MiCAR within the definition of Article 3, 1. (9), due to the necessity “exclusively” being intended to provide access to a good or a service supplied by its issuer only.

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 WLFI tokens referred to in this white paper are crypto-assets other than EMTs and ARTs, and are issued on the Ethereum, Solana and BNB Smart Chain network (2025-09-26 and according to DTI FFG shown in F.14).

The first activity on Ethereum can be viewed on 2024-09-29 (see https://etherscan.io/tx/0x707e076245ca1860a063879615d9b4e924fb33d6f5f39c78416037a16735f4cc).

The first activity on BNB Smart Chain can be viewed on 2025-09-01 (see https://bscscan.com/tx/0xae2972fd2d48eb8088a69556666149e7427504a9726c54f0bbdd6aebc96da8a7).

The first activity on Solana can be viewed on 2025-08-23 (see https://solscan.io/tx/2gxaD8FQhpdU2ng6VothgRvNfVZ8xV7j7wWB7zhjmMmoeYatimgA7YEWqXDY6zcUuuuWLzufJp1CW2iguiWa7wJs).

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

Not applicable.

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

Crypto Risk Metrics GmbH is seeking admission to trading on any Crypto Asset Service Provider platform in the European Union in accordance to Article 5 of REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. In accordance to Article 5(4), this crypto-asset white paper may be used by entities admitting the token to trading after Crypto Risk Metrics GmbH as the person responsible for drawing up such white paper has given its consent to its use in writing to the repective Crypto Asset Service Provider. If a CASP wishes to use this white paper, inquiries can be made under info@crypto-risk-metrics.com.

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

A.1 Name

Crypto Risk Metrics GmbH

A.2 Legal form

2HBR

A.3 Registered address

DE, Lange Reihe 73, 20099 Hamburg, Germany

A.4 Head office

Not applicable.

A.5 Registration date

2018-12-03

A.6 Legal entity identifier

39120077M9TG0O1FE242

A.7 Another identifier required pursuant to applicable national law

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

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

030

A.11 Parent company

Not applicable.

A.12 Members of the management body

Name	Position	Address

Tim Zölitz	Chairman	Lange Reihe 73, 20099 Hamburg, Germany

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider, who supports regulated entities in the fulfillment of their regulatory requirements. In this regard, Crypto Risk Metrics GmbH acts as a data-provider for ESG-data according to article 66 (5). Due to the regulations laid out in article 5 (4) of the REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, Crypto Risk Metrics GmbH aims at providing central services for crypto-asset white papers in order to minimize market confusion due to conflicting white papers for the same asset.

A.14 Parent company business activity

Not applicable.

A.15 Newly established

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

A.16 Financial condition for the past three years

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

2024 (unaudited): negative 50.891,81 EUR

2023 (unaudited): negative 27.665,32 EUR

2022: 104.283,00 EUR.

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

A.17 Financial condition since registration

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

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

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

Yes

B.2 Name

According to the information disclosed in the official "Gold Paper" (available at https://static.worldlibertyfinancial.com/docs/intl/gold-paper.pdf, accessed 2025-10-06) and the issuer's website, the entity World Liberty Financial, Inc., described as a Delaware non-stock corporation, appears to be the principal legal person responsible for the operation, maintenance, and governance of the World Liberty Financial protocol. Based on the data available at the date of this document, and in the absence of independently verifiable alternative information, it is most likely that this Delaware non-stock corporation constitutes the issuer within the meaning of the applicable regulatory framework.

The Gold Paper indicates that the corporation administers the WLFI governance process and holds contractual relationships with several affiliated or associated entities, including but not limited to DT Marks DeFi LLC, Axiom Management Group (AMG), and other service providers that perform operational, promotional, or technical functions on behalf of the project. The precise corporate interrelationships, contractual hierarchy, and distribution of responsibilities among these entities are not transparently disclosed and cannot be independently verified.

It must also be noted that, based on the issuer's own documentation and widely reported public records, the network of associated companies and contractual beneficiaries includes or has been connected to politically exposed persons ("PEPs"),

particularly in relation to Donald J. Trump and his affiliated business organizations. The Gold Paper expressly refers to the granting of rights to use personal likeness, name, and related publicity rights of Donald Trump as part of the promotional framework. As a result, these associations introduce a heightened level of regulatory, reputational, and political risk.

B.3 Legal form

XTIQ

B.4. Registered address

According to the information disclosed in the official filing submitted to the U.S. Securities and Exchange Commission (SEC) on 03 July 2025 (Form D, Filer ID 0002043140) World Liberty Financial, Inc. is incorporated in the United States of America, with its registered address stated as:

US-DE – 407 Ayre Street, Suite #1358, Wilmington, Delaware 19804, United States.

B.5 Head office

Could not be found while drafting this white paper (2025-09-29).

B.6 Registration date

2024-10-30, according to the information disclosed in the official filing submitted to the U.S. Securities and Exchange Commission (SEC) on 03 July 2025 (Form D, Filer ID 0002043140).

B.7 Legal entity identifier

Could not be found while drafting this white paper (2025-10-02).

B.8 Another identifier required pursuant to applicable national law

CIK number: 0002043140

B.9 Parent company

According to the information made publicly available on the issuer's website, WLF Holdco LLC may not be formally designated as the parent company of World Liberty

Financial, Inc. under corporate law; however, it is reportedly entitled to receive distributions, revenue shares, or other financial interests arising from the activities of the issuing entity. In the absence of transparent ownership disclosures, it must therefore be assumed that WLF Holdco LLC exercises a level of economic influence comparable to that of a parent or controlling company. The precise ownership structure and control relationships have not been independently verified, and consequently, the legal and financial interdependence between WLF Holdco LLC and World Liberty Financial, Inc. remains uncertain.

B.10 Members of the management body

Name	Position	Business address
Info	The following information is based exclusively on the data disclosed in the official filing submitted to the U.S. Securities and Exchange Commission (SEC). It lists only those individuals who are formally identified in the filing as Directors or Executive Officers of World Liberty Financial, Inc. However, it is acknowledged that a number of additional persons are publicly associated with the broader project and promotional campaigns of World Liberty Financial, as reflected in section D.5 of this document. The precise scope of involvement and actual influence of all related individuals cannot be independently verified beyond the information contained in the SEC filing. Consequently, the extent of their decision-making authority or operational control within the project remains uncertain and	Not applicable.

	may differ from the formal titles or roles indicated in regulatory disclosures.	
Zachary Folkman	Executive Officer & Director	US-PR – 425 Carr 693 PMB 285, Dorado, Puerto Rico 00646, United States
Chase Herro	Executive Officer & Director	US-DE – 407 Ayre Street, PMB #1358, Wilmington, Delaware 19805, United States

B.11 Business activity

"Other technology", according to the information disclosed in the official filing submitted to the U.S. Securities and Exchange Commission (SEC) on 03 July 2025 (Form D, Filer ID 0002043140) .

B.12 Parent company business activity

Could not be found while drafting this white paper (2025-09-29).

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

C.1 Name

Not applicable.

C.2 Legal form

Not applicable.

C.3 Registered address

Not applicable.

C.4 Head office

Not applicable.

C.5 Registration date

Not applicable.

C.6 Legal entity identifier

Not applicable.

C.7 Another identifier required pursuant to applicable national law

Not applicable.

C.8 Parent company

Not applicable.

C.9 Reason for crypto-Asset white paper Preparation

Not applicable.

C.10 Members of the Management body

Not applicable.

C.11 Operator business activity

Not applicable.

C.12 Parent company business activity

Not applicable.

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

Not applicable.

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

Not applicable.

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "World Liberty Financial", Short Name: "WLFI" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-09-26).

D.2 Crypto-assets name

See F.13.

D.3 Abbreviation

See F.13.

D.4 Crypto-asset project description

World Liberty Financial ("WLFI") is presented by its promoters as a decentralized finance (DeFi) initiative designed to integrate elements of traditional financial infrastructure with blockchain-based governance. According to the publicly accessible project materials (including the "Gold Paper" and the website https://worldlibertyfinancial.com, accessed 2025-10-05), the ecosystem is built around two core components:

- the WLFI governance token, intended to enable participation in protocol-level decision-making; and

- USD1, a purportedly U.S.-dollar-backed stablecoin meant to facilitate transactions within the network.

The project documentation suggests that WLFI aims to create a hybrid financial environment connecting traditional markets and digital assets through tokenized governance and asset issuance mechanisms. However, these objectives remain unverified and lack external auditing or regulatory confirmation. The publicly available

information does not provide a verifiable technical white paper, code repository, or audited smart-contract documentation.

The project has gained significant public attention due to its association with politically exposed individuals (PEPs) and entities linked to prominent public figures. Such affiliations introduce elevated regulatory, reputational, and compliance risks, as the project's operations may be influenced by political or non-commercial considerations. The potential for changes in political circumstances, public perception, or regulatory response presents a material risk to the project's sustainability and token value.

From a functional perspective, WLFI is described as a governance token that grants holders the ability to vote on ecosystem-related proposals. Nevertheless, these governance rights do not appear to confer any enforceable legal entitlements or ownership interests. Participation in governance is therefore discretionary and dependent on the issuer's or foundation's continued operation and goodwill.

As of the date of this white paper, no detailed or binding roadmap has been published, and future project milestones are based solely on third-party interpretations and media statements that cannot be independently verified. The absence of transparent disclosures, audited financial data, or confirmed governance mechanisms significantly limits investors' ability to assess the long-term viability of the project.

Given the combination of political exposure, concentrated control, and limited public accountability, WLFI must be regarded as a high-risk crypto-asset project. Prospective investors should exercise heightened due diligence and recognize that the information available from public sources may be incomplete, outdated, or subject to material change without prior notice.

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

Name	Position	Business address
Info	The following information is based exclusively on the data disclosed in the official filing submitted	Not applicable.

	to the U.S. Securities and Exchange Commission (SEC). It lists only those individuals who are formally identified in the filing as Directors or Executive Officers of World Liberty Financial, Inc. However, it is acknowledged that a number of additional persons are publicly associated with the broader project and promotional campaigns of World Liberty Financial, as reflected in section D.5 of this document. The precise scope of involvement and actual influence of all related individuals cannot be independently verified beyond the information contained in the SEC filing. Consequently, the extent of their decision-making authority or operational control within the project remains uncertain and may differ from the formal titles or roles indicated in regulatory disclosures.	
Zachary Folkman	Executive Officer & Director of the Issuer	US-PR – 425 Carr 693 PMB 285, Dorado, Puerto Rico 00646, United States
Chase Herro	Executive Officer & Director Director of the Issuer	US-DE – 407 Ayre Street, PMB #1358, Wilmington, Delaware 19805, United States

World Liberty Financial, Inc.	Issuer	US-DE – 407 Ayre Street, PMB #1358, Wilmington, Delaware 19805, United States
Donald John Trump	Promoter of the issuer	US-FL – 115 Eagle Tree Terrace, Jupiter, Florida 33477, United States
Eric Trump	Promoter of the issuer	US-FL – 115 Eagle Tree Terrace, Jupiter, Florida 33477, United States
Steven Witkoff	Promoter of the issuer	US-FL – 4400 Biscayne Boulevard, Suite 900, Miami, Florida 33137, United States
Zachary Wittkoff	Promoter of the issuer	US-FL – 4400 Biscayne Boulevard, Suite 900, Miami, Florida 33137,

		United States
Axiom Management Group LLC	Promoter of the issuer	US-PR – 425 Carr 693 PMB 285, Dorado, Puerto Rico 00646, United States
WC DigitalFi LLC	Promoter of the issuer	US-FL – 4400 Biscayne Boulevard, Suite 900, Miami, Florida 33137, United States
DT Marks DEFI, LLC	Promoter of the issuer	US-FL – 115 Eagle Tree Terrace, Jupiter, Florida 33477, United States
Justin Sun	According to third parties, Justin Sun invested in WLFI (https://www.reuters.com/business/finance/how-trump-family-took-over-crypto-firm-it-raised-hundreds-millions-2025-03-31, accessed 2025-10-06)	Can not be found
WLF Holdco LLC	WLF Holdco LLC is referenced in publicly available information and media reports as an entity associated with World Liberty Financial, Inc.. While its exact corporate function and	Can not be found

	ownership structure are not fully disclosed, it is reportedly entitled to receive distributions or other financial interests from the issuer's operations. Although it may not be formally designated as a parent company, its role and economic relationship suggest that it may exercise influence comparable to that of a controlling or holding entity.	
Disclaimer	Due to the high degree of structural opacity and the particular political exposure of several individuals involved in the project, it cannot be excluded that additional relevant relationships or persons may exist that are not publicly disclosed or identifiable through available sources. This lack of transparency constitutes a significant risk factor for investors, as undisclosed affiliations or external influences could materially affect the governance, operation, or economic performance of the project.	Not applicable

D.6 Utility Token Classification

The token does not classify as a utility token.

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

Not applicable.

D.8 Plans for the token

According to the publicly available materials (including the "Gold Paper" published on https://worldlibertyfinancial.com, accessed 2025-10-05), the development of the WLFI token has followed several identifiable historical milestones. The project was first

announced in early 2024 as a decentralized finance initiative intended to merge elements of traditional finance and blockchain governance. In mid-2024, the issuer began the initial token sales, which reportedly raised several hundred million U.S. dollars from public and private rounds. During this period, the WLFI token was introduced as a non-transferable governance token.

In early 2025, the community approved, through a governance vote, the activation of WLFI transferability - allowing tokenholders to trade and transfer WLFI on secondary markets. This was followed by listings on major centralized exchanges in September 2025, marking the official start of open market trading.

Beyond these past events, no official roadmap or binding development plan has been published by the issuer. While certain third-party sources and community discussions have referred to potential future developments - such as the introduction of a WLFI-linked debit card, integration of lending and borrowing features, and the tokenization of real-world assets - none of these prospective milestones have been independently verified or confirmed by the project itself. The published information is fragmentary, largely promotional, and lacks verifiable implementation timelines or technical documentation.

As a result, investors should be aware that there is no authoritative or externally audited roadmap for WLFI. The absence of clear, binding commitments regarding future functionality or strategic direction creates significant uncertainty concerning the token's long-term development, governance evolution, and potential market value. Any third-party statements about future plans must therefore be considered aspirational and speculative in nature.

Accordingly, the future value, functionality, and adoption of WLFI will depend primarily on external market conditions, community participation, and discretionary decisions by the issuer or its governance structure. There is no guarantee that the project will achieve any of its publicly mentioned objectives, and the token's performance may be highly sensitive to regulatory, political, and reputational developments.

D.9 Resource allocation

According to the publicly available documentation (including the "Gold Paper" published on https://worldlibertyfinancial.com, accessed 2025-10-05), the total supply of the $WLFI token is fixed at 100,000,000,000 units. The project's stated allocation framework divides this supply across several categories intended to support governance, ecosystem growth, and community participation. Based on the information contained in the referenced documentation and secondary data aggregators, approximately 35% of the total supply has been designated for public and private token sales, providing the principal source of financial resources allocated to the project's development. A further 32.5% has been assigned to community and ecosystem incentives, including liquidity programs, adoption campaigns, and protocol reward mechanisms. Around 30% of the total supply has been reserved for early adopters, while approximately 2.5% is allocated to team members and advisors.

It must be emphasized that the figures and vesting arrangements described above originate solely from publicly accessible materials provided by the project and third-party data platforms and have not been independently verified. The actual implementation of these allocations, unlock schedules, and vesting terms may differ from what is stated in these sources.

The temporary token distribution can be traced on-chain, on Ethereum: https://etherscan.io/token/0xda5e1988097297dcdc1f90d4dfe7909e847cbef6#balances .

The temporary token distribution can be traced on-chain, on BNB Smart Chain: https://bscscan.com/token/0x47474747477b199288bF72a1D702f7Fe0Fb1DEeA#balances.

The temporary token distribution can be traced on-chain, on Solana: https://solscan.io/token/WLFinEv6ypjkczcS83FZqFpgFZYwQXutRbxGe7oC16g#holders.

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

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

Not applicable, as this white paper was drawn up for the admission to trading and not for collecting funds for the crypto-asset-project.

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

E.1 Public offering or admission to trading

The white paper concerns the admission to trading (i. e. ATTR) on any Crypto Asset Service Providers platform that has obtained the written consent of Crypto Risk Metrics GmbH as the person drafting this white paper.

E.2 Reasons for public offer or admission to trading

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

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The crypto-asset project itself refers to a total supply of 100,000,000,000 units (https://static.worldlibertyfinancial.com/docs/intl/gold-paper.pdf, accessed 2025-10-03). Investors should note that changes in the token supply can have a negative impact.

The effective amount of tokens available on the market depends on the number of tokens released by the issuer or other parties at any given time, as well as potential reductions through token "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

ALL

E.14 Holder restrictions

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

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

Not applicable.

E.31 CASP identifier

Not applicable.

E.32 Placement form

Not applicable.

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

Not applicable.

E.35 Trading platforms access

This depends on the trading platform listing the asset.

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCAR) but does not qualify as an electronic money token (EMT) or an asset-referenced token (ART). It is a digital representation of value that can be stored and transferred using distributed ledger technology (DLT) or similar technology, without embodying or conferring any rights to its holder.

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

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

F.2 Crypto-asset functionality

According to the publicly available documentation provided by the issuer (including the "Gold Paper" accessible via https://worldlibertyfinancial.com, accessed 2025-10-05), the $WLFI token is described as a governance token within the World Liberty Financial ecosystem. The token is intended to enable holders to participate in on-chain governance processes, including voting on protocol proposals, liquidity strategies, and token-related decisions such as buy-back or burn mechanisms.

However, it must be explicitly emphasized that none of the described functionalities can be independently verified or are guaranteed to be implemented as stated. The governance rights referenced in public communications and marketing materials do not appear to confer any enforceable legal rights or claims against the issuer, the project entity, or any associated undertaking. The ability of WLFI holders to effectively exercise such governance rights depends on the technical and contractual implementation of the protocol, which has not been independently audited or confirmed by third parties.

Furthermore, WLFI does not appear to grant any form of ownership, profit participation, or redemption rights. The token's functionality is thus of a purely discretionary nature, dependent on the issuer's or governance body's decisions. The legal status of the governance framework and the binding nature of tokenholder votes remain uncertain under applicable law.

Consequently, investors must be aware that the practical and legal realization of any claimed functionalities, rights, or use cases of WLFI is subject to material uncertainty. Participation in governance or ecosystem activities may not guarantee any enforceable outcomes, and the token's effective functionality may differ substantially from its

described purpose. The investor bears the full risk that such functionalities may not materialize or may later be altered or revoked.

F.3 Planned application of functionalities

See D.8.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

The tokens are crypto-assets other than EMTs and ARTs, which are available on the Ethereum, Solana and BNB Smart Chain blockchain. The tokens are fungible (up to 18 on Ethereum and BNB Smart Chain and 6 digits on Solana after the decimal point). The tokens are a digital representation of value, and have no inherent rights attached as well as no intrinsic utility.

F.7 Commercial name or trading name

See F.13.

F.8 Website of the issuer

https://worldlibertyfinancial.com/

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

2025-11-03

F.10 Publication date

2025-11-03

F.11 Any other services provided by the issuer

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

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

EN

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

H50D9HB3K; J75VP8MPH; ZLZ08WV6N

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

3XVWCVFSX

F.15 Voluntary data flag

Mandatory.

F.16 Personal data flag

The white paper does contain personal data.

F.17 LEI eligibility

The issuer should be eligible for a Legal Entity Identifier.

F.18 Home Member State

Germany

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

G.2 Exercise of rights and obligations

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

G.3 Conditions for modifications of rights and obligations

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

G.4 Future public offers

Information on the future offers to the public of crypto-assets were not available at the time of writing this white paper (2025-09-28).

G.5 Issuer retained crypto-assets

According to the publicly available documentation (including the "Gold Paper" published on https://worldlibertyfinancial.com, accessed 2025-10-05), the total supply of the $WLFI token is fixed at 100,000,000,000 units. The project's stated allocation framework divides this supply across several categories intended to support governance, ecosystem growth, and community participation. Based on the information contained in the referenced documentation and secondary data aggregators, approximately 35% of the total supply has been designated for public and private token sales, providing the principal source of financial resources allocated to the project's development. A further 32.5% has been assigned to community and ecosystem incentives, including liquidity programs, adoption campaigns, and protocol reward mechanisms. Around 30% of the

total supply has been reserved for early adopters, while approximately 2.5% is allocated to team members and advisors.

It must be emphasized that the figures and vesting arrangements described above originate solely from publicly accessible materials provided by the project and third-party data platforms and have not been independently verified. The actual implementation of these allocations, unlock schedules, and vesting terms may differ from what is stated in these sources.

According to the allocation framework, approximately 2.5% of the total WLFI supply has been assigned to team members and advisors, which can be regarded as clearly issuer-retained. In addition, around 30% of the supply has been reserved for early adopters, a category that likely includes entities and individuals closely affiliated with the project during its initial development phase. Furthermore, about 32.5% of the tokens have been allocated to ecosystem and community incentives, a portion of which may remain under discretionary control of the issuer or its governance structures.

Taking these categories together, and under a conservative interpretation, it can be assumed that between 33% and 45% of the total token supply could be regarded as issuer-retained in the broader sense. This estimate reflects potential economic control rather than legal ownership and is subject to material uncertainty.

The temporary token distribution can be traced on-chain, on Ethereum: https://etherscan.io/token/0xda5e1988097297dcdc1f90d4dfe7909e847cbef6#balances .

The temporary token distribution can be traced on-chain, on BNB Smart Chain: https://bscscan.com/token/0x47474747477b199288bF72a1D702f7Fe0Fb1DEeA#balances.

The temporary token distribution can be traced on-chain, on Solana: https://solscan.io/token/WLFinEv6ypjkczcS83FZqFpgFZYwQXutRbxGe7oC16g#holders.

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

G.6 Utility token classification

No

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

Not applicable.

G.8 Utility tokens redemption

Not applicable.

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No, there are no fixed protocols that can increase or decrease the supply implemented as of 2025-09-16. Nevertheless, it is possible that the owner of the smart-contract has the ability to increase or decrease the token-supply in response to changes in demand. Also, it is possible to decrease the circulating supply, by transferring crypto-assets to so

called "burn-adresses", which are adresses that render the crypto-asset "non-transferable" after sent to those adresses.

G.13 Supply adjustment mechanisms

The mint authority (the entity who can create new tokens of that crypto-asset), has the potential right to change the supply of the crypto-assets. The official website states, that the maximum supply is capped at the maximum of 100,000,000,000 (https://static.worldlibertyfinancial.com/docs/intl/gold-paper.pdf, accessed 2028-09-28). Investors should note that changes in the token supply can have a negative impact.

G.14 Token value protection schemes

No, the token does not have value protection schemes.

G.15 Token value protection schemes description

Not applicable.

G.16 Compensation schemes

No, the token does not have compensation schemes.

G.17 Compensation schemes description

Not applicable.

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

See F.13.

H.2 Protocols and technical standards

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana, Ethereum and BNB Smart Chain. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Solana:

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

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

Core functions of the Token Program:

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

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

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

transfer() → Transfers tokens between accounts

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

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

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

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

The following applies to Ethereum:

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

1. Network Protocols

The crypto-asset follows a decentralized, peer-to-peer (P2P) protocol where nodes communicate over the crypto-asset's DevP2P protocol using RLPx for data encoding.

- Transactions and smart contract execution are secured through Proof-of-Stake (PoS) consensus.

- Validators propose and attest blocks in Ethereum's Beacon Chain, finalized through Casper FFG.

- The Ethereum Virtual Machine (EVM) executes smart contracts using Turing-complete bytecode.

2. Transaction and Address Standards

crypto-asset Address Format: 20-byte addresses derived from Keccak-256 hashing of public keys.

Transaction Types:

- Legacy Transactions (pre-EIP-1559)

- Type 0 (Pre-EIP-1559 transactions)

- Type 1 (EIP-2930: Access list transactions)

- Type 2 (EIP-1559: Dynamic fee transactions with base fee burning)

The Pectra upgrade introduces EIP-7702, a transformative improvement to account abstraction. This allows externally owned accounts (EOAs) to temporarily act as smart contract wallets during a transaction. It provides significant flexibility, enabling functionality such as sponsored gas payments and batched operations without changing the underlying account model permanently.

3. Blockchain Data Structure & Block Standards

- the crypto-asset's blockchain consists of accounts, smart contracts, and storage states, maintained through Merkle Patricia Trees for efficient verification.

Each block contains:

- Block Header: Parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, proposer signature.

- Transactions: Smart contract executions and token transfers.

- Block Size: No fixed limit; constrained by the gas limit per block (variable over time). In line with Ethereum’s scalability roadmap, Pectra includes EIP-7691, which increases the maximum number of "blobs" (data chunks introduced with EIP-4844) per block. This change significantly boosts the data availability layer used by rollups, supporting cheaper and more efficient Layer 2 scalability.

4. Upgrade & Improvement Standards

Ethereum follows the Ethereum Improvement Proposal (EIP) process for upgrades.

The following applies to BNB Smart Chain:

Binance Smart Chain (BSC) is a Layer-1 blockchain that utilizes a Proof-of-Staked Authority (PoSA) consensus mechanism. This mechanism combines elements of Proof-of-Authority (PoA) and Proof-of-Stake (PoS) and is intended to secure the network and validate transactions. In PoSA, validators are selected based on their stake and authority, with the goal of providing fast transaction times and low fees while maintaining network security through staking.

H.3 Technology used

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana, Ethereum and BNB Smart Chain. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Solana:

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

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

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

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

Security Protocols for Asset Custody and Transactions:

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

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

The following applies to Ethereum:

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

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

3. Cryptographic Integrity: Ethereum employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers. The Keccak-256 (SHA-3 variant) Hashing Algorithm is used for hashing and address generation. The crypto-asset uses ECDSA with secp256k1 curve for key generation and digital signatures. Next to that, BLS (Boneh-Lynn-Shacham) signatures are used for validator aggregation in PoS.

The following applies to BNB Smart Chain:

1. BSC-Compatible Wallets

Tokens on BSC are supported by wallets compatible with the Ethereum Virtual Machine (EVM), such as MetaMask. These wallets can be configured to connect to the BSC network and are designed to interact with BSC using standard Web3 interfaces.

2. Ledger

BSC maintains its own decentralized ledger for recording token transactions. This ledger is intended to ensure transparency and security, providing a verifiable record of all activities on the network.

3. BEP-20 Token Standard

BSC supports tokens implemented under the BEP-20 standard, which is tailored for the BSC ecosystem. This standard is designed to facilitate the creation and management of tokens on the network.

4. Scalability and Transaction Efficiency

BSC is designed to handle high volumes of transactions with low fees. It leverages its PoSA consensus mechanism to achieve fast transaction times and efficient network performance, making it suitable for applications requiring high throughput.

H.4 Consensus mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana, Ethereum and BNB Smart Chain. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Solana:

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

Core Concepts

1. Proof of History (PoH):

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

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

2. Proof of Stake (PoS):

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

selected to validate transactions and produce new blocks.

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

cryptographic clock for the network.

3. Block Production:

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

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

4. Consensus and Finalization:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

The following applies to Ethereum:

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

The following applies to BNB Smart Chain:

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof of Staked Authority (PoSA), which combines elements of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA). This method ensures fast block times and low fees while maintaining a level of decentralization and security. Core Components 1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security. 2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security. 3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a

crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process 4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes. 5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network. 6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives 7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB. 8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance. 9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

H.5 Incentive mechanisms and applicable fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana, Ethereum and BNB Smart Chain. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

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

2. Rent Fees:

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

3. Smart Contract Fees:

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

The following applies to Ethereum:

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity.

The following applies to BNB Smart Chain:

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators. Incentive Mechanisms 1. Validators: Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks. 2. Delegators: Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network's security and decentralization by choosing reliable validators. 3. Candidates: Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience. 4. Economic Security: Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network. Opportunity Cost: Staking requires validators and delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets. Fees on the Binance Smart Chain 5. Transaction Fees: Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators. Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet. 6. Block Rewards: Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions. 7. Cross-Chain Fees: Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal

fees, facilitating seamless asset transfers and improving user experience. 8. Smart Contract Fees: Deployment and Execution Costs: Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

H.6 Use of distributed ledger technology

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

H.7 DLT functionality description

Not applicable.

H.8 Audit

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

H.9 Audit outcome

Not applicable.

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Operational and Technical

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

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

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

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

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

3. Market and Liquidity

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

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

4. Counterparty

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

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

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

5. Liquidity

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

6. Failure of one or more Counterparties

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

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

7. Information asymmetry

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

I.2 Issuer-related risks

1. Insolvency

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

2. Counterparty

In order to operate, entities involved in the project have most likely engaged in different business relationships with one or more third parties on which they and the network strongly depend on. Loss or changes in the leadership or key partners of entities involved in the project and/or the respective counterparties can lead to disruptions, loss

of trust, or project failure. This could result in a total loss of economic value for the crypto-asset holders.

3. Legal and Regulatory Compliance

Cryptocurrencies and blockchain-based technologies are subject to evolving regulatory landscapes worldwide. Regulations vary across jurisdictions and may be subject to significant changes. Non-compliance can result in investigations, enforcement actions, penalties, fines, sanctions, or the prohibition of the trading of the crypto-asset impacting its viability and market acceptance. This could also result in entities involved in the project to be subject to private litigation. The aforeementioned would most likely also lead to changes with respect to trading of the crypto-asset that may negatively impact the value, legality, or functionality of the crypto-asset.

4. Operational

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

5. Industry

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

6. Reputational

The network and all entities involved in the project face the risk of negative publicity, whether due to, without limitation, operational failures, security breaches, or association with illicit activities, which can damage the reputation of the network and all entities involved in the project and, by extension, the value and acceptance of the crypto-asset.

7. Competition

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

8. Unanticipated Risk

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

9. Political exposure and concentration of influence

The World Liberty Financial project is publicly associated with individuals who hold, or have held, prominent political positions, as well as with entities perceived to be closely connected to politically exposed persons ("PEPs"). Such affiliations may expose the project to heightened legal, regulatory, and reputational risks. In particular, political exposure may increase the likelihood of regulatory scrutiny, sanctions risk, or future restrictions imposed by supervisory authorities in certain jurisdictions.

Moreover, the concentration of influence in the hands of founders or affiliates with significant public visibility creates a potential asymmetry of information and decision-making power between tokenholders and the project's core controllers. Decisions regarding token issuance, governance, treasury management, or public communications may be shaped by non-commercial or politically motivated considerations, which can adversely affect the token's value, governance neutrality, and long-term sustainability.

Investors should also be aware that political developments affecting such individuals - including election outcomes, changes in office, sanctions, or public controversies - could materially impact the perception, market access, or even the operational continuity of the project. The reputational linkage between the crypto-asset and its politically exposed founders represents a non-quantifiable but material risk that may lead to volatility, exclusion from regulated markets, or termination of service relationships (e.g., with exchanges or custodians).

I.3 Crypto-assets-related risks

1. Valuation

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

2. Market Volatility

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

3. Liquidity Challenges

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

4. Asset Security

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

5. Scams

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

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

6. Blockchain Dependency

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

7. Smart Contract Vulnerabilities

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

8. Privacy Concerns

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

9. Regulatory Uncertainty

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

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

10. Counterparty risk

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

11. Reputational concerns

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

12. Technological Innovation

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

13. Community and Narrative

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

14. Interest Rate Change

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

15. Taxation

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

16. Anti-Money Laundering/Counter-Terrorism Financing

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

17. Market Abuse

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

18. Timeline and Milestones

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

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

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

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

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

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

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

I.4 Project implementation-related risks

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

I.5 Technology-related risks

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

1. Blockchain Dependency Risks

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

2. Smart Contract Risks

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

3. Wallet and Storage Risks

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

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

4. Network Security Risks

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

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

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

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

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

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

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

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

I.6 Mitigation measures

None.

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

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

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the cryptoasset

World Liberty Financial

S.4 Consensus Mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana, Ethereum and BNB Smart Chain. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Solana:

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

Core Concepts

1. Proof of History (PoH):

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

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

2. Proof of Stake (PoS):

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

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

Consensus Process

1. Transaction Validation:

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

2. PoH Sequence Generation:

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

cryptographic clock for the network.

3. Block Production:

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

4. Consensus and Finalization:

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

Security and Economic Incentives

1. Incentives for Validators:

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

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

2. Security:

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

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

3. Economic Penalties:

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

The following applies to Ethereum:

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

The following applies to BNB Smart Chain:

Binance Smart Chain (BSC) uses a hybrid consensus mechanism called Proof of Staked Authority (PoSA), which combines elements of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA). This method ensures fast block times and low fees while

maintaining a level of decentralization and security. Core Components 1. Validators (so-called “Cabinet Members”): Validators on BSC are responsible for producing new blocks, validating transactions, and maintaining the network’s security. To become a validator, an entity must stake a significant amount of BNB (Binance Coin). Validators are selected through staking and voting by token holders. There are 21 active validators at any given time, rotating to ensure decentralization and security. 2. Delegators: Token holders who do not wish to run validator nodes can delegate their BNB tokens to validators. This delegation helps validators increase their stake and improves their chances of being selected to produce blocks. Delegators earn a share of the rewards that validators receive, incentivizing broad participation in network security. 3. Candidates: Candidates are nodes that have staked the required amount of BNB and are in the pool waiting to become validators. They are essentially potential validators who are not currently active but can be elected to the validator set through community voting. Candidates play a crucial role in ensuring there is always a sufficient pool of nodes ready to take on validation tasks, thus maintaining network resilience and decentralization. Consensus Process 4. Validator Selection: Validators are chosen based on the amount of BNB staked and votes received from delegators. The more BNB staked and votes received, the higher the chance of being selected to validate transactions and produce new blocks. The selection process involves both the current validators and the pool of candidates, ensuring a dynamic and secure rotation of nodes. 5. Block Production: The selected validators take turns producing blocks in a PoA-like manner, ensuring that blocks are generated quickly and efficiently. Validators validate transactions, add them to new blocks, and broadcast these blocks to the network. 6. Transaction Finality: BSC achieves fast block times of around 3 seconds and quick transaction finality. This is achieved through the efficient PoSA mechanism that allows validators to rapidly reach consensus. Security and Economic Incentives 7. Staking: Validators are required to stake a substantial amount of BNB, which acts as collateral to ensure their honest behavior. This staked amount can be slashed if validators act maliciously. Staking incentivizes validators to act in the network's best interest to avoid losing their staked BNB. 8. Delegation and Rewards: Delegators earn rewards proportional to their stake in validators. This incentivizes them to choose reliable validators and participate in the

network's security. Validators and delegators share transaction fees as rewards, which provides continuous economic incentives to maintain network security and performance. 9. Transaction Fees: BSC employs low transaction fees, paid in BNB, making it cost-effective for users. These fees are collected by validators as part of their rewards, further incentivizing them to validate transactions accurately and efficiently.

S.5 Incentive Mechanisms and Applicable Fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Solana, Ethereum and BNB Smart Chain. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to Solana:

1. Validators:

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

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

2. Delegators:

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

3. Economic Security:

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

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

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

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

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

2. Rent Fees:

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

3. Smart Contract Fees:

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

The following applies to Ethereum:

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity.

The following applies to BNB Smart Chain:

Binance Smart Chain (BSC) uses the Proof of Staked Authority (PoSA) consensus mechanism to ensure network security and incentivize participation from validators and delegators. Incentive Mechanisms 1. Validators: Staking Rewards: Validators must stake a significant amount of BNB to participate in the consensus process. They earn rewards in the form of transaction fees and block rewards. Selection Process: Validators are selected based on the amount of BNB staked and the votes received from delegators. The more BNB staked and votes received, the higher the chances of being selected to validate transactions and produce new blocks. 2. Delegators: Delegated Staking: Token holders can delegate their BNB to validators. This delegation increases the validator's total stake and improves their chances of being selected to produce blocks. Shared Rewards: Delegators earn a portion of the rewards that validators receive. This incentivizes token holders to participate in the network’s security and decentralization by choosing reliable validators. 3. Candidates: Pool of Potential Validators: Candidates are nodes that have staked the required amount of BNB and are waiting to become active validators. They ensure that there is always a sufficient pool of nodes ready to take on validation tasks, maintaining network resilience. 4. Economic Security: Slashing: Validators can be penalized for malicious behavior or failure to perform their duties. Penalties include slashing a portion of their staked tokens, ensuring that validators act in the best interest of the network. Opportunity Cost: Staking requires validators and

delegators to lock up their BNB tokens, providing an economic incentive to act honestly to avoid losing their staked assets. Fees on the Binance Smart Chain 5. Transaction Fees: Low Fees: BSC is known for its low transaction fees compared to other blockchain networks. These fees are paid in BNB and are essential for maintaining network operations and compensating validators. Dynamic Fee Structure: Transaction fees can vary based on network congestion and the complexity of the transactions. However, BSC ensures that fees remain significantly lower than those on the Ethereum mainnet. 6. Block Rewards: Incentivizing Validators: Validators earn block rewards in addition to transaction fees. These rewards are distributed to validators for their role in maintaining the network and processing transactions. 7. Cross-Chain Fees: Interoperability Costs: BSC supports cross-chain compatibility, allowing assets to be transferred between Binance Chain and Binance Smart Chain. These cross-chain operations incur minimal fees, facilitating seamless asset transfers and improving user experience. 8. Smart Contract Fees: Deployment and Execution Costs: Deploying and interacting with smart contracts on BSC involves paying fees based on the computational resources required. These fees are also paid in BNB and are designed to be cost-effective, encouraging developers to build on the BSC platform.

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

2024-10-03

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

2025-10-03

S.8 Energy consumption

3096.35814 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 Ethereum, Solana and BNB Smart Chain 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

32.2255486008 %

S.11 Energy intensity

0.00004 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

1.03051 tCO2e/a

S.14 GHG intensity

0.00001 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal energy cost wrt. one more transaction. Ember (2025); Energy Institute -

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

S.16 Key GHG sources and methodologies

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

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.