White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG RW7GP3S5G

Preamble

00. Table of Contents

01. Date of notification 11

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

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

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

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

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

Summary 12

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

08. Characteristics of the crypto-asset 12

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

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

Part A – Information about the offeror or the person seeking admission to trading 14

A.1 Name 14

A.2 Legal form 14

A.3 Registered address 14

A.4 Head office 14

A.5 Registration date 14

A.6 Legal entity identifier 14

A.7 Another identifier required pursuant to applicable national law 14

A.8 Contact telephone number 14

A.9 E-mail address 14

A.10 Response time (Days) 14

A.11 Parent company 15

A.12 Members of the management body 15

A.13 Business activity 15

A.14 Parent company business activity 16

A.15 Newly established 16

A.16 Financial condition for the past three years 16

A.17 Financial condition since registration 16

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading 17

B.1 Issuer different from offeror or person seeking admission to trading 17

B.2 Name 17

B.3 Legal form 17

B.4. Registered address 17

B.5 Head office 17

B.6 Registration date 17

B.7 Legal entity identifier 17

B.8 Another identifier required pursuant to applicable national law 17

B.9 Parent company 17

B.10 Members of the management body 17

B.11 Business activity 17

B.12 Parent company business activity 18

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 18

C.1 Name 18

C.2 Legal form 18

C.3 Registered address 18

C.4 Head office 18

C.5 Registration date 18

C.6 Legal entity identifier 18

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

C.8 Parent company 18

C.9 Reason for crypto-Asset white paper Preparation 19

C.10 Members of the Management body 19

C.11 Operator business activity 19

C.12 Parent company business activity 19

C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 19

C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 19

Part D – Information about the crypto-asset project 19

D.1 Crypto-asset project name 19

D.2 Crypto-assets name 19

D.3 Abbreviation 19

D.4 Crypto-asset project description 20

D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project 20

D.6 Utility Token Classification 25

D.7 Key Features of Goods/Services for Utility Token Projects 26

D.8 Plans for the token 26

D.9 Resource allocation 27

D.10 Planned use of Collected funds or crypto-Assets 28

Part E – Information about the offer to the public of crypto-assets or their admission to trading 29

E.1 Public offering or admission to trading 29

E.2 Reasons for public offer or admission to trading 29

E.3 Fundraising target 29

E.4 Minimum subscription goals 29

E.5 Maximum subscription goals 29

E.6 Oversubscription acceptance 29

E.7 Oversubscription allocation 29

E.8 Issue price 29

E.9 Official currency or any other crypto-assets determining the issue price 30

E.10 Subscription fee 30

E.11 Offer price determination method 30

E.12 Total number of offered/traded crypto-assets 30

E.13 Targeted holders 30

E.14 Holder restrictions 30

E.15 Reimbursement notice 30

E.16 Refund mechanism 31

E.17 Refund timeline 31
E.18 Offer phases 31
E.19 Early purchase discount 31
E.20 Time-limited offer 31
E.21 Subscription period beginning 31
E.22 Subscription period end 31
E.23 Safeguarding arrangements for offered funds/crypto- Assets 31
E.24 Payment methods for crypto-asset purchase 32
E.25 Value transfer methods for reimbursement 32
E.26 Right of withdrawal 32
E.27 Transfer of purchased crypto-assets 32
E.28 Transfer time schedule 32
E.29 Purchaser's technical requirements 32
E.30 Crypto-asset service provider (CASP) name 32
E.31 CASP identifier 32
E.32 Placement form 32
E.33 Trading platforms name 33
E.34 Trading platforms Market identifier code (MIC) 33
E.35 Trading platforms access 33
E.36 Involved costs 33
E.37 Offer expenses 33
E.38 Conflicts of interest 33
E.39 Applicable law 33
E.40 Competent court 33
Part F – Information about the crypto-assets 34

F.1 Crypto-asset type 34

F.2 Crypto-asset functionality 34

F.3 Planned application of functionalities 35

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 36

F.4 Type of crypto-asset white paper 36

F.5 The type of submission 36

F.6 Crypto-asset characteristics 36

F.7 Commercial name or trading name 36

F.8 Website of the issuer 36

F.9 Starting date of offer to the public or admission to trading 36

F.10 Publication date 36

F.11 Any other services provided by the issuer 36

F.12 Language or languages of the crypto-asset white paper 37

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 37

F.14 Functionally fungible group digital token identifier, where available 37

F.15 Voluntary data flag 37

F.16 Personal data flag 37

F.17 LEI eligibility 37

F.18 Home Member State 37

F.19 Host Member States 37

Part G – Information on the rights and obligations attached to the crypto-assets 37

G.1 Purchaser rights and obligations 37

G.2 Exercise of rights and obligations 38
G.3 Conditions for modifications of rights and obligations 38
G.4 Future public offers 38
G.5 Issuer retained crypto-assets 39
G.6 Utility token classification 40
G.7 Key features of goods/services of utility tokens 40
G.8 Utility tokens redemption 40
G.9 Non-trading request 41
G.10 Crypto-assets purchase or sale modalities 41
G.11 Crypto-assets transfer restrictions 41
G.12 Supply adjustment protocols 41
G.13 Supply adjustment mechanisms 41
G.14 Token value protection schemes 41
G.15 Token value protection schemes description 41
G.16 Compensation schemes 41
G.17 Compensation schemes description 42
G.18 Applicable law 42
G.19 Competent court 42
Part H – information on the underlying technology 42
H.1 Distributed ledger technology (DTL) 42
H.2 Protocols and technical standards 42
H.3 Technology used 45
H.4 Consensus mechanism 47
H.5 Incentive mechanisms and applicable fees 51
H.6 Use of distributed ledger technology 55

H.7 DLT functionality description 55

H.8 Audit 55

H.9 Audit outcome 55

Part I – Information on risks 55

I.1 Offer-related risks 55

I.2 Issuer-related risks 57

I.3 Crypto-assets-related risks 59

I.4 Project implementation-related risks 63

I.5 Technology-related risks 63

I.6 Mitigation measures 65

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts 65

J.1 Adverse impacts on climate and other environment-related adverse impacts 65

S.1 Name 65

S.2 Relevant legal entity identifier 65

S.3 Name of the cryptoasset 65

S.4 Consensus Mechanism 66

S.5 Incentive Mechanisms and Applicable Fees 70

S.6 Beginning of the period to which the disclosure relates 73

S.7 End of the period to which the disclosure relates 73

S.8 Energy consumption 73

S.9 Energy consumption sources and methodologies 73

S.10 Renewable energy consumption 74

S.11 Energy intensity 74

S.12 Scope 1 DLT GHG emissions – Controlled 74

S.13 Scope 2 DLT GHG emissions – Purchased 74

S.14 GHG intensity 74

S.15 Key energy sources and methodologies 74

S.16 Key GHG sources and methodologies 75

01. Date of notification

2025-12-22

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 Sidekick 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 (2025-10-30 and according to DTI FFG shown in F.14) with a total number of 1,000,000,000 token.

The first activity on Ethereum can be viewed on 2025-08-05 (see https://etherscan.io/tx/0x9c08a9facfaaf2c6f7e26a7e958a3f49675dbe75e8fda80b42c940281220165c),

on Solana on 2025-08-05 (see https://solscan.io/tx/4CmGFd3LAz7qxTAqwrBDcEi7byAJaJ9r9dve7cJa6ExrFyYP1opm3kbupSmTWw9ATkadRYP3bgKin5XNuheqmTwc) and on BNB Smart Chain 2025-08-05 (see https://bscscan.com/tx/0x2e6b1764ec4d9ae9a3a7e8c3269d8142069071ce74d5be58a0d7da7e769a17d0).

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

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

Not applicable.

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

This white paper concerns the admission to trading of the crypto-asset "Sidekick" by "Hub Development Foundation" 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.

The following platforms are in scope for this while drafting up this white paper: Payward Global Solutions Limited. Further platforms are also being sought for this purpose in the future.

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

A.1 Name

Hub Development Foundation

A.2 Legal form

UNCO

A.3 Registered address

PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

A.4 Head office

PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

A.5 Registration date

2024-11-13

A.6 Legal entity identifier

Not available.

A.7 Another identifier required pursuant to applicable national law

25059099

A.8 Contact telephone number

+44 7518042681

A.9 E-mail address

panamafoundation@sidekick.fans

A.10 Response time (Days)

030

A.11 Parent company

Not applicable.

A.12 Members of the management body

Name	Position	Address
Diana Muñoz	President, Council Member	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Omar Camargo	Secretary, Council Member	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Persis Manfred Sarmiento	Treasurer, Council Member	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

A.13 Business activity

Hub Development Foundation is a non-profit private interest foundation incorporated in Panama. Its principal function is to act as the legal issuer of the token, ensuring compliance with applicable regulatory frameworks and safeguarding the token issuance process. The Foundation is entrusted with managing the token generation event (TGE),

allocation of tokens according to vesting schedules, and treasury governance in connection with the initial issuance.

Following the completion of the token issuance, and in accordance with protocol arrangements, the responsibility for long-term development, ecosystem growth, and ongoing protocol governance will transition to Sidekick Foundation, which will act as the steward of the Sidekick Protocol and its LiveFi ecosystem.

Hub Development Foundation will therefore remain primarily as the legal steward of token-related responsibilities, while Sidekick Foundation will carry forward development and operational activities.

A.14 Parent company business activity

Not applicable.

A.15 Newly established

Yes

A.16 Financial condition for the past three years

Not applicable.

A.17 Financial condition since registration

The issuing entity was established in 2024 and has therefore not yet completed three full financial years of operation.

Since inception, the Foundation has focused on establishing the Sidekick Protocol's core infrastructure, securing strategic partnerships, and deploying initial operational funding. No material adverse changes or unusual events have occurred that would significantly affect the Foundation's financial position since registration.

Key financial indicators, including total funding raised (approximately USD 11 million), cumulative expenditures (~USD 5.27 million), and remaining treasury (~USD 2.07 million), reflects the project's early-stage development and prudent capital allocation. The Foundation continues to maintain short- and medium-term liquidity sufficient to sustain operations for an estimated 13 months at the current expenditure rate.

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

No

B.2 Name

Not applicable.

B.3 Legal form

Not applicable.

B.4. Registered address

Not applicable.

B.5 Head office

Not applicable.

B.6 Registration date

Not applicable.

B.7 Legal entity identifier

Not applicable.

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Not applicable.

B.11 Business activity

Not applicable.

B.12 Parent company business activity

Not applicable.

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

C.1 Name

Not applicable.

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: "Sidekick", Short Name: "K" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-10-19).

D.2 Crypto-assets name

Long Name: "Sidekick"

D.3 Abbreviation

Short Name: "K"

D.4 Crypto-asset project description

The Sidekick Protocol is a blockchain-based live-streaming infrastructure designed to facilitate real-time content monetisation and audience interaction through the use of its native token. The protocol enables creators and users to participate in on-chain engagement mechanisms such as tipping, gifting and community-driven interactions. These functions are executed through verifiable and transparent processes, ensuring that participation and value transfer remain traceable on-chain.

The system applies a "LiveFi" model, under which live-stream interactions are recorded and settled using decentralised technology, allowing users to engage directly with creators while maintaining a reliable and tamper-resistant record of activity. The project is structured to provide an infrastructure layer that supports compliant, transparent and sustainable forms of digital engagement within a decentralised environment.

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

Name	Position	Address
Diana Muñoz	President, Council Member (Issuer)	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Omar Camargo	Secretary, Council Member (Issuer)	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

Persis Manfred Sarmiento	Treasurer, Council Member (Issuer)	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Hub Development Foundation	Issuer	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Sidekick Foundation	Ecosystem supporter	KY - 3119, 9 Forum Lane, Camana Bay, George Town, Grand Cayman KY1-9006
Jasmine	Advisor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Adam	Advisor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

Yu Hu	Investor and Advisor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Anthony Cheng	Advisor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
YZi Labs	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Initial Ventures Fund LP	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Mable	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica,

		Panama City, Republic of Panama
Mirana Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Piers Kicks (HuxCo Limited)	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Y2Z Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Yu Hu (Kaito.ai)	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
HashKey Capital	Investor	PA - Oceania Business Plaza, 21st Floor, Tower

		1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Folius Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Manifold Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Foresight Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Fenbushi Capital	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

Altos Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
CEIC (Yiren Digital Ltd.)	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Animoca Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama
Crit Ventures	Investor	PA - Oceania Business Plaza, 21st Floor, Tower 1000, Isaac Hanono Missri Street, Punta Pacifica, Panama City, Republic of Panama

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

The development of the Sidekick Protocol and the associated token follows a structured, phased roadmap aimed at establishing a compliant LiveFi infrastructure and progressively expanding the token's functional scope. The project's evolution combines technical implementation, compliance validation and ecosystem expansion, undertaken with a focus on operational reliability and regulatory conformity.

Past milestones:

From Q1 2024 onwards, the project focused on building the foundation of the Sidekick platform and validating its operational processes. In Q1 2024, the Sidekick WebApp was launched with integrated off-chain payment gateways, including USDT and third-party processors, accompanied by initial compliance testing related to transaction routing and payment flows. In Q2 2024, the project released a Discord Mini App, extending compliant order processing by leveraging integrated third-party gateways.

During Q3 and Q4 2024, a strategic transition began toward a LiveFi-based streaming infrastructure, requiring substantial adjustments to the compliance framework, back-end architecture and general protocol design. In Q1 2025, the project conducted a closed beta phase to validate live-streaming infrastructure, user authentication processes and compliance workflows. During this period, a smart contract audit and AML procedures were finalised, and platform access was opened under the approved compliance model.

In Q2 2025, tipping and gifting functionalities were activated with on-chain monitoring to ensure compliant execution. In Q3 2025, the Token Generation Event (TGE) was completed, and the corresponding smart contract was deployed. In Q4 2025, the MiCA white paper was finalised and submitted.

Future Milestones

For 2026, the project plans to integrate the token into platform transaction fee mechanisms and expand token-based access features that support non-financial

participation. In 2027, the protocol aims to introduce governance participation modules based on non-financial on-chain voting and to implement premium access tiers designed to broaden the token's utility within the Sidekick ecosystem. These developments are intended to extend the operational functionality of the token without conferring ownership, profit participation, or revenue rights.

D.9 Resource allocation

The total supply is divided across several predefined allocation categories intended to structure the long-term distribution of resources within the Sidekick ecosystem. These categories represent the planned framework for how tokens may be deployed over time and are not, in themselves, indicative of the circulating supply at the Token Generation Event (TGE). Each allocation category is subject to a vesting schedule designed to support gradual release and controlled distribution.

According to the current allocation model, 20 % of the supply is attributed to Investors, subject to a 12-month cliff followed by linear vesting over 24 months, with no tokens released at TGE. A further 20 % is allocated to Ecosystem Growth, intended to support development and expansion of the protocol; this category foresees approximately one-third of its allocation becoming available at TGE under a short cliff and extended linear vesting.

20 % is assigned to Long-Term Community Incentives to support user participation, creator engagement, and ecosystem programmes, with a limited initial release and a multi-year vesting timeline. The Liquidity Incentive category represents 4 % of supply and is structured to facilitate liquidity provisioning, with half of its allocation made available at TGE and the remainder subject to a short vesting period.

In addition, 5 % is allocated to Advisors, with no tokens released at TGE and distribution occurring only after a 12-month cliff followed by linear vesting. The Foundation allocation comprises 16 %, subject to a six-month cliff and subsequent vesting to support operational continuity and ecosystem stewardship. Finally, 15 % is allocated to Core Contributors, also featuring a 12-month cliff and extended linear vesting.

This allocation structure defines the categories under which tokens are intended to be distributed over time. It does not determine the timing or actual release of tokens into circulation beyond the vesting logic applicable to each category. At the time of the TGE, only a limited portion of the allocated supply becomes transferable, resulting in an initial circulating proportion of approximately 11.13 %. Subsequent increases in circulating supply will occur gradually according to cliff periods, linear vesting mechanisms, operational requirements and compliance considerations.

Actual utilisation of allocated resources may deviate from initial plans due to technical, organisational or regulatory factors. Furthermore, vesting events, redistributions or market-level transfers may affect the circulating supply and influence the token's distribution over time.

The temporary token distribution can be traced on-chain on Ethereum:

https://etherscan.io/token/0xfb072b42907dA2Bf7A8E8cB5dCAa790D45Fd81a8#balances

On Solana:

https://solscan.io/token/ERpDpYmuifJUKbaB1Dv9hnJ67RM21Jujmxz18JCeDzbr#holders

On BNB Smart Chain:

https://bscscan.com/token/0x0a73d885cdd66adf69c6d64c0609e55c527db2be#balances

Investors must be aware that a public blockchain address cannot necessarily be attributed to a single natural or legal person, which limits the ability to determine exact economic influence or future actions. Changes in escrow releases or market-level redistributions may affect the circulating supply and could have an impact on the token's market value.

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).

E.2 Reasons for public offer or admission to trading

The crypto asset is to be listed on the platforms: Payward Global Solutions Limited. Additional platforms aren't excluded in the future.

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 maximum supply of the crypto-asset is set at 1,000,000,000 units. 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

Payward Global Solutions Limited. Other platforms are also planned for future listing.

E.34 Trading platforms Market identifier code (MIC)

Payward Global Solutions Limited: PGSL

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 addressing, 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

At the time of listing (August 2025), the token serves as a functional unit within the Sidekick Protocol and is designed to facilitate participation in live-stream interactions. Its primary operational purpose is to enable users to provide on-chain rewards to creators through gifting and tipping mechanisms, thereby supporting real-time engagement and creator monetisation within the LiveFi model. These interactions are settled on-chain and recorded in a transparent and verifiable manner.

The functionality of the token at this stage is limited to these engagement-related use cases and does not grant holders any ownership, profit, revenue, or similar financial rights. Further technical capabilities may be added in later development phases of the protocol; however, these future functionalities are not active at the time of listing and do not alter the non-financial nature of the token's current functionality.

F.3 Planned application of functionalities

The functionalities associated with the token will be introduced in a phased manner as the Sidekick Protocol undergoes further technical development. The following applications are planned to become available in subsequent stages of the project's rollout:

Transaction Fees (Planned 2025–2026):

The token is planned to be introduced as a medium for paying transaction fees within the Sidekick Protocol. This will apply to on-chain interactions such as digital asset trading and other LiveFi-related ecosystem functions.

Governance Participation (Planned 2026):

Token holders are expected to obtain the ability to participate in non-financial, on-chain governance processes. These mechanisms will allow users to provide input on protocol parameters, feature configurations and ecosystem-related decisions. Governance rights will not include ownership, profit-sharing, or revenue entitlements.

Token-Based Access and Participation Benefits (Planned 2026):

Holding and using tokens is planned to enable non-monetary benefits such as enhanced platform functionalities, additional interface customisation options and eligibility for selected creator or community participation programmes within the Sidekick ecosystem.

Premium Access Tiers (Planned 2026–2027):

The project foresees the introduction of premium access levels through which token holders may obtain early access to certain content, advanced engagement features and curated platform experiences.

These planned functionalities are intended solely to expand the operational and participatory utility of the token within the Sidekick Protocol and do not confer any ownership, financial claims, or rights to participate in profits or revenues.

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 network. The tokens are fungible (up to 18 digits after the decimal point on Ethereum and BNB Smart Chain and 9 on Solana). 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

Sidekick

F.8 Website of the issuer

https://sidekick.fans/

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

2026-01-23

F.10 Publication date

2026-01-23

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

3MN2W2XR3; 74VD3JXHN; L2RTHRSQT

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

RW7GP3S5G

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

Ireland

F.19 Host Member States

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

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

G.1 Purchaser rights and obligations

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

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

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

G.2 Exercise of rights and obligations

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

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

G.3 Conditions for modifications of rights and obligations

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

Adjustments to the technical protocol, smart contract logic, or related systems may occur in the ordinary course of development or maintenance.

Such changes do not alter any legal position of holders, as no contractual or regulatory rights exist. Holders should not interpret technical updates or governance-related changes as amendments to legally binding entitlements.

G.4 Future public offers

This white paper refers to admission to trading. The issuer reserves the right to make further offers in the future. This means that future public offers cannot be ruled out, although there are no current plans to do so.

G.5 Issuer retained crypto-assets

The total supply is divided across several predefined allocation categories intended to structure the long-term distribution of resources within the Sidekick ecosystem. These categories represent the planned framework for how tokens may be deployed over time and are not, in themselves, indicative of the circulating supply at the Token Generation Event (TGE). Each allocation category is subject to a vesting schedule designed to support gradual release and controlled distribution.

According to the current allocation model, 20 % of the supply is attributed to Investors, subject to a 12-month cliff followed by linear vesting over 24 months, with no tokens released at TGE. A further 20 % is allocated to Ecosystem Growth, intended to support development and expansion of the protocol; this category foresees approximately one-third of its allocation becoming available at TGE under a short cliff and extended linear vesting.

20 % is assigned to Long-Term Community Incentives to support user participation, creator engagement, and ecosystem programmes, with a limited initial release and a multi-year vesting timeline. The Liquidity Incentive category represents 4 % of supply and is structured to facilitate liquidity provisioning, with half of its allocation made available at TGE and the remainder subject to a short vesting period.

In addition, 5 % is allocated to Advisors, with no tokens released at TGE and distribution occurring only after a 12-month cliff followed by linear vesting. The Foundation allocation comprises 16 %, subject to a six-month cliff and subsequent vesting to support operational continuity and ecosystem stewardship. Finally, 15 % is allocated to Core Contributors, also featuring a 12-month cliff and extended linear vesting.

This allocation structure defines the categories under which tokens are intended to be distributed over time. It does not determine the timing or actual release of tokens into circulation beyond the vesting logic applicable to each category. At the time of the TGE, only a limited portion of the allocated supply becomes transferable, resulting in an initial circulating proportion of approximately 11.13 %. Subsequent increases in circulating supply will occur gradually according to cliff periods, linear vesting mechanisms, operational requirements and compliance considerations.

Actual utilisation of allocated resources may deviate from initial plans due to technical, organisational or regulatory factors. Furthermore, vesting events, redistributions or market-level transfers may affect the circulating supply and influence the token's distribution over time.

At the time of writing this white paper, 862,600,000 tokens can be considered as issuer-retained.

The temporary token distribution can be traced on-chain on Ethereum:

https://etherscan.io/token/0xfb072b42907dA2Bf7A8E8cB5dCAa790D45Fd81a8#balances

On Solana:

https://solscan.io/token/ERpDpYmuifJUKbaB1Dv9hnJ67RM21Jujmxz18JCeDzbr#holders

On BNB Smart Chain:

https://bscscan.com/token/0x0a73d885cdd66adf69c6d64c0609e55c527db2be#balances

Investors must be aware that a public blockchain address cannot necessarily be attributed to a single natural or legal person, which limits the ability to determine exact economic influence or future actions. Changes in escrow releases or market-level redistributions may affect the circulating supply and could have an impact on the token's market value.

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 2025-10-17. Also, it is possible to decrease the circulating supply, by transferring crypto-assets to so called "burn-addresses", which are addresses that render the crypto-asset "non-transferable" after sent to those addresses.

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 1,000,000,000 tokens. 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)

The crypto asset in scope will be implemented on the DLT network Ethereum, Solana and BNB Smart Chain as a token, following the standards described below.

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: Ethereum, Solana 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 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 Solana:

The tokens are 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 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: Ethereum, Solana 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 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 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 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: Ethereum, Solana 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 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 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 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: Ethereum, Solana 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 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 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 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.

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.

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 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

Hub Development Foundation

S.2 Relevant legal entity identifier

Not applicable.

S.3 Name of the cryptoasset

Sidekick

S.4 Consensus Mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Ethereum, Solana 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 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 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 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: Ethereum, Solana 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 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 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 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

2024-10-28

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

2025-10-28

S.8 Energy consumption

395.90855 kWh/a

S.9 Energy consumption sources and methodologies

The energy consumption of this asset is aggregated across multiple components: To determine the energy consumption of a token, the energy consumption of the networks 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

33.1320248670 %

S.11 Energy intensity

0.00000 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.13506 tCO2e/a

S.14 GHG intensity

0.00000 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are 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.