IKA WHITE PAPER

IN ACCORDANCE WITH TITLE II OF REGULATION (EU) 2023/1114

00 TABLE OF CONTENT

01 DATE OF NOTIFICATION

2025-07-21

Compliance Statements

02 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 This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 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 The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05 The utility token referred to in this white paper may not be exchangeable against the good or service promised in the crypto-asset white paper, especially in the case of a failure or discontinuation of the crypto-asset project.

06 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.

The crypto-asset referred to in this white paper is not covered by the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

07 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 (36) or any other offer document pursuant to Union or national law.

08 Characteristics of the crypto-asset

The IKA token is a crypto-asset as defined by article 3(1)(5) of the Markets in Crypto-Assets Regulation (EU) 2013/1114 ('MiCA').

Symbol: IKA

Initial supply: 10,000,000,000 tokens

Blockchain platform: Sui

Token Standard: Sui Move Coin Standard

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

More specifically, IKA is a utility token pursuant to Article 3(1)(9) of the Markets in Crypto-Assets Regulation (MiCA). This token enables holders to participate in the Ika network by facilitating cryptographic operations, conducting protocol-level transactions such as staking and signing, and engaging in decentralized governance. Collectively, these functionalities support the Ika decentralized MPC network.

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

The Ika Foundation is seeking admission to trading of the IKA token on multiple trading platforms.

PART I – INFORMATION ON RISKS

I.1 Offer-Related Risks

The person seeking admission to trading of the crypto-asset neither operates, controls, oversees, nor manages the functioning of the Exchanges where the Token will be admitted. Additionally, the Token's underlying protocol and governance structure may evolve due to ongoing technical, regulatory, and industry developments. Unforeseen risks may arise, and new challenges or opportunities may necessitate changes in the Network's strategies, goals, and structure. The risks outlined below highlight regulatory uncertainty, liquidity limitations, governance risks, network centralization concerns, security vulnerabilities, and potential adjustments to fees or token supply that could impact the offer and trading of the Token.

Regulatory Compliance Risks: Although the Token is designed to comply with existing regulations (such as MiCA), evolving regulatory landscapes could impact its classification, trading status, or market acceptance. Changes in regulatory requirements may necessitate modifications to the Network's operation, structure, or governance. Purchasers must ensure compliance with local laws, as regulatory treatment of crypto-assets varies across jurisdictions.

Market Volatility: The Token is subject to extreme price fluctuations, influenced by speculation, market sentiment, and broader industry trends. External factors, such as regulatory announcements or technological developments, may further contribute to volatility, potentially leading to financial losses for holders.

Liquidity Risks: The ability to buy and sell Tokens depends on trading activity on decentralized exchanges ("DEXs") and, if applicable, centralized exchanges ("CEXs"). Limited liquidity may result in difficulties executing large trades without significant price impact, increasing the risk of loss.

Risk of Trading Platforms: When Token holders trade on Exchanges, the person seeking admission to trading of the crypto-asset does not act as a contractual party to these transactions. All legal relationships regarding these trading platforms are subject to their respective terms and conditions, with no responsibility assumed by the person seeking admission to trading of the crypto-asset for their operations, services, or outcomes.

Risk of Delisting: There is no guarantee that the Token will remain listed on any exchange. Delisting could significantly hinder the ability to trade Tokens, reducing liquidity and market value.

Risk of Bankruptcy: The Exchanges or trading platforms where the Token is listed may become insolvent or cease operations, potentially resulting in a loss of access to funds or Tokens.

Blockchain and Smart Contract Dependency: The Token relies entirely on its blockchain infrastructure. Any network downtime, congestion, security vulnerabilities, or smart contract failures could negatively impact its functionality, accessibility, or security. Additionally, the Network may initially operate under a centralized or permissioned model, where specific node operators manage the network. This structure presents centralization risks, including the potential for censorship or data monetization.

Governance and Economic Model Risks: The current model relies on inflation. However, governance decisions or operational needs may necessitate future adjustments, potentially increasing inflationary mechanisms or modifications to the fee structure.

Operational Risks: Risks associated with the person seeking admission to trading of the crypto-asset's internal processes, personnel, and technologies may impact the ability to manage the Token's operations effectively. Failures in operational integrity could lead to disruptions, financial losses, or reputational damage.

Financial Risks: The person seeking admission to trading of the crypto-asset may face financial risks, including liquidity shortages, credit risks, or market fluctuations, which could affect its ability to continue operations, meet obligations, or sustain the stability and value of the Token.

Legal Risks: Uncertainties in legal frameworks, regulatory changes, potential lawsuits, or adverse legal rulings could pose significant risks, affecting the legality, usability, or value of the Token.

Fraud and Mismanagement Risks: The risk of fraudulent activity or mismanagement within the person seeking admission to trading of the crypto-asset's operations may impact the credibility of the project and the usability or value of the Token.

Reputational Risks: Negative publicity—whether due to operational failures, security breaches, or associations with illicit activities—could damage the person seeking admission to trading of the crypto-asset's reputation and, by extension, impact the value and acceptance of the Token.

Technology Management Risks: Inadequate management of technological updates or failure to keep pace with advancements may result in security vulnerabilities, inefficiencies, or obsolescence of the Token and its supporting infrastructure.

Dependency on Key Individuals: The success of the Token and its ecosystem may be highly dependent on key individuals. Loss or changes in project leadership could lead to operational disruptions, a loss of trust, or potential project failure.

Conflicts of Interest: Misalignment of interests between the person seeking admission to trading of the crypto-asset and Token holders may lead to governance decisions that are not in the best interests of the community, potentially affecting the value of the Token or damaging the credibility of the project.

Counterparty Risks: The person seeking admission to trading of the crypto-asset's reliance on external partners, service providers, and collaborators introduces risks related to non-fulfilment of obligations, which may affect the Token's operations, liquidity, or overall ecosystem stability.

Industry Competition Risks: The person seeking admission to trading of the crypto-asset faces competition from other projects, including larger and well-funded ventures that may attract more users and liquidity, potentially diminishing the viability of the Token.

Speculative Nature of the Token: Other than as stated herein with respect to the rights, functions, or other utilities that may be introduced by governance votes, the Token has no inherent utility beyond market sentiment and community driven interest. Its value is highly speculative and subject to fluctuations based on external perceptions.

Unanticipated Risks: There may be additional risks that cannot be foreseen. Some risks may materialize as unexpected variations or combinations of the factors discussed in this section.

I.2 Issuer-Related Risks

Regulatory Compliance Risks: Issuers of crypto assets must adhere to a wide array of regulatory requirements across different jurisdictions. Non-compliance can result in fines, sanctions, or the prohibition of the crypto asset offering, impacting its viability and market acceptance.

Operational Risks: These include risks related to the issuer's internal processes, personnel, and technologies, which can affect their ability to manage crypto-asset operations effectively. Failures in operational integrity might lead to disruptions, financial losses, or reputational damage.

Financial Risks: Issuers face financial risks, including liquidity, credit, and market risks. These could affect the issuer's ability to continue operations, meet obligations, or sustain the stability or value of the crypto-asset.

Legal Risks: Legal uncertainties, potential lawsuits, or adverse legal rulings can pose significant risks to issuers. Legal challenges may affect the legality, usability, or value of a crypto-asset.

Fraud and Mismanagement Risks: There is a risk of fraudulent activity or mismanagement by the issuer, which can lead to directly impacting the usability or value of a crypto-asset or damage the credibility of the project.

Reputational Risks: Negative publicity, whether due to operational failures, security breaches, or association with illicit activities, can damage an issuer's reputation and, by extension, the value and acceptance of the crypto-asset.

Technology Management Risks: Inadequate management of technological updates or failure to keep pace with technological advancements can render a crypto-asset, or the project it is connected to, obsolete or vulnerable to security risks.

Dependency on Key Individuals: The success of some crypto projects can be highly dependent on the expertise and leadership of key individuals. Loss or changes in the project's leadership can lead to disruptions, loss of trust, or project failure.

Conflicts of Interest: Risks arise when the issuer's interests do not align with those of the crypto-asset holders, potentially leading to decisions that are not in the best interests of the asset holders, impacting the value of a crypto-asset or damage the credibility of the project.

Counterparty Risks: Risks associated with the issuer's partners, suppliers, or collaborators, including the potential for non-fulfillment of obligations that can affect the issuer's operations.

I.3 Crypto-Assets-Related Risks

Market Risk: Crypto-assets are notoriously volatile, with prices subject to significant fluctuations due to market sentiment, regulatory news, technological advancements, and macroeconomic factors.

Liquidity Risk: Some crypto-assets may suffer from low liquidity, making it difficult to buy or sell large amounts without affecting the market price, which could lead to significant losses, especially in fast-moving market conditions.

Custodial Risk: Risks associated with the theft of crypto-assets from exchanges or wallets, loss of private keys, or failure of custodial services, which can result in the irreversible loss of crypto-assets.

Smart Contract Risk: Crypto-assets might be connected to or be issued with the help of smart contracts. Smart contracts are code running on a blockchain, executing the programmed functions automatically if the defined conditions are fulfilled. Bugs or vulnerabilities in smart contract code can expose blockchain users to potential hacks and exploits. Any flaw in the code can lead to unintended consequences, such as the loss of crypto-assets or unauthorized access to sensitive data.

Regulatory and Tax Risk: Changes in the regulatory environment for crypto-assets (such as consumer protection, taxation, and anti-money laundering requirements) could affect the use, value, or legality of crypto-assets in a given jurisdiction.

Counterparty Risk: In cases where crypto-assets are used in contractual agreements or held on exchanges, there is a risk that the counterparty may fail to fulfill their obligations due to insolvency, compliance issues, or fraud, resulting in loss of crypto-assets.

Reputational Risk: Association with illicit activities, high-profile thefts, or technological failures can damage the reputation of certain crypto-assets, impacting user trust and market value.

I.4 Project Implementation-Related Risks

The person seeking admission to trading of the crypto-asset neither operates, controls, oversees, nor manages the technology underlying the Ecosystem. While efforts are made to ensure security and stability, blockchain-based technologies are still evolving, and various risks exist. Additionally, the success and sustainability of the project rely on various external factors, including market conditions, regulatory developments, and technological advancements.

Technical Development Risks:

Smart Contract Issues: Despite robust security measures, unforeseen vulnerabilities or bugs in the smart contracts could disrupt project's implementation and functionality.

Blockchain Dependency: The Token operates exclusively on its underlying blockchain. Any network congestion, downtime, or security breaches could impact the project's implementation and functionality.

Risk of Security Weaknesses in Core Infrastructure: The project relies on open-source software, which may be modified by third parties not directly affiliated with the person seeking admission to trading of the crypto-asset. Weaknesses or bugs introduced into the core infrastructure could compromise security and lead to the loss of digital assets. Furthermore, malfunctions or inadequate maintenance of the Network may negatively impact the Token's usability.

Bugs in Core Blockchain Code: Even with rigorous testing, unknown bugs may exist in the blockchain protocol, potentially leading to disruptions, incorrect transaction processing, or security vulnerabilities.

Regulatory and Compliance Risks:

Regulatory Actions in One or More Jurisdictions: The Token and the underlying Network could be impacted by regulatory inquiries or actions, which may restrict further development, implementation, or usage.

Evolving Laws and Regulations: New and changing laws related to financial securities, consumer protection, data privacy, cybersecurity, and intellectual property could impact the project. Compliance with these laws may require significant resources and could impose additional operational constraints.

Governance Risks:

Network Governance Risks: Decision-making mechanisms in blockchain governance may be inefficient, slow, or disproportionately influenced by specific stakeholders, leading to potential centralization or unfavourable network changes.

Consensus Failures or Forks: Errors in the consensus mechanism could lead to forks, where multiple versions of the ledger coexist, or network halts, reducing trust in the network.

Operational Risks: The project's success depends on allocating sufficient resources (both financial and non-financial) to ensure timely development and deployment. Poor resource management could lead to delays or failure to achieve key milestones.

Market Adoption Risks:

Competitive Environment: The crypto market is highly competitive and trend-driven. There is a risk that the Token may fail to capture sufficient interest, limiting its adoption.

Community Engagement Risks: The success of the Token depends heavily on community-driven marketing and engagement. Failure to build or sustain an active community could hinder growth and long-term tradability.

7. **Timeline and Milestone Risks**:

Delayed Milestones: Key deliverables such as Token distribution, liquidity bootstrapping, and market-making efforts may face delays due to technical, operational, or funding challenges.

CEX Listing Risks: Listings on centralized exchanges depend on securing the necessary funding for listing fees and meeting platform-specific requirements. Delays or insufficient resources could postpone broader market access.

Ecosystem Risks:

Dependence on External Partners: The project relies on partnerships with infrastructure providers, exchanges, and other third-party service providers. Any failure or delay from these partners could disrupt implementation plans.

Risk of Withdrawing Partners: The Token holder understands that the feasibility of the project depends strongly on the collaboration of service providers and other key stakeholders. A loss of critical partnerships could impact project sustainability.

Technology and Software Risks:

Risk of Software Weakness: The Token holder acknowledges that blockchain and smart contract technologies are still evolving. There is no guarantee that Token usage will be uninterrupted or error-free. Vulnerabilities in the underlying blockchain, smart contracts, or supporting technologies could lead to the complete loss of Tokens or their functionality.

Dependency on Underlying Technology: The project relies on blockchain infrastructure, hardware, and network connectivity, all of which may be subject to failures, outages, or vulnerabilities.

Risk of Technological Disruption: The emergence of new technology, such as quantum computing, could undermine the security of blockchain encryption and compromise the integrity of digital assets.

Unforeseen Bugs and Security Vulnerabilities: The Token and its supporting infrastructure rely on blockchain technologies that may still be evolving. There is no guarantee that Token transactions will be uninterrupted or error-free. Software vulnerabilities, weaknesses in smart contracts, or infrastructure issues may result in loss of assets, security breaches, or unexpected network failures.

Network Security Risks:

Risk of Security Weaknesses in the Network's Core Infrastructure Software: The Website, Services, and the Network operate with open-source software. There is a risk that third parties not directly affiliated with the Ika Foundation may introduce weaknesses or bugs into the core infrastructural elements, leading to loss or harm to digital assets.

Network Attacks and Cybersecurity Threats: Blockchain networks can be vulnerable to cyberattacks such as 51% attacks, Sybil attacks, or distributed denial-of-service ("DDoS") attacks. These threats could disrupt network operations and compromise security.

Blockchain Network Attacks: The Network may be subject to mining attacks, including double-spend attacks, reorganizations, majority mining power attacks, "vampire" attacks, "selfish-mining" attacks, and work race condition attacks. Successful attacks could compromise the proper execution of transactions and smart contracts.

Privacy and Anonymity Risks: Blockchain transactions are recorded on a public ledger, which may expose transaction history and financial activity. Certain transactions could be linked to specific wallet addresses, making users vulnerable to fraud, phishing attacks, or targeted scams.

Economic and Governance Risks:

Economic Self-Sufficiency: The long-term sustainability of the Token ecosystem depends on sufficient transaction volume to support validator incentives and maintain network security. A lack of adoption could lead to governance-driven changes to monetary policy, fee structures, or consensus mechanisms.

Incentive Model Risks: Changes to block rewards, staking incentives, or governance models may be required to maintain network participation. Governance decisions could result in modifications that impact Token holders, including inflationary adjustments, transaction fees, or redistribution of rewards.

Unanticipated Risks: In addition to the risks identified, new threats may emerge due to changes in legal, technological, or economic conditions. Developments such as regulatory crackdowns, unforeseen Network vulnerabilities, or disruptive innovations could impact the usability, security, or value of the Token in ways not currently foreseeable.

I.5 Technology-Related Risks

Private Key Management Risk and Loss of Access to Crypto-Assets: The security of crypto-assets heavily relies on the management of private keys, which are used to access and control the crypto-assets (e.g. initiate transactions). Poor management practices, loss, or theft of private keys, or respective credentials, can lead to irreversible loss of access to crypto-assets.

Settlement and Transaction Finality: By design, a blockchain's settlement is probabilistic, meaning there is no absolute guaranteed finality for a transaction. There remains a theoretical risk that a transaction could be reversed or concurring versions of the ledger could persist due to exceptional circumstances such as forks or consensus errors. The risk diminishes as more blocks are added, making it increasingly secure over time. Under normal circumstance, however, once a transaction is confirmed, it cannot be reversed or cancelled. Crypto-assets sent to a wrong address cannot be retrieved, resulting in the loss of the sent crypto assets.

Scaling Limitations and Transaction Fees: As the number of users and transactions grows, a blockchain network may face scaling challenges. This could lead to increased transaction fees and slower transaction processing times, affecting usability and costs.

Economic Self-sufficiency and Operational Parameters: A blockchain network might not reach the critical mass in transaction volume necessary to sustain self-sufficiency and remain economically viable to incentivize block production. In failing to achieve such inflection point, a network might lose its relevance, become insecure, or result in changes to the protocol's operational parameters, such as the monetary policy, fee structure and consensus rewards, governance model, or technical specifications such as block size or intervals.

Network Attacks and Cyber Security Risks: Blockchain networks can be vulnerable to a variety of cyber-attacks, including 51% attacks, where an attacker gains control of the majority of the network's consensus, Sybil attacks, or DDoS attacks. These can disrupt the network's operations and compromise data integrity, affecting its security and reliability.

Consensus Failures or Forks: Faults in the consensus mechanism can lead to forks, where multiple versions of the ledger coexist, or network halts, potentially destabilizing the network and reducing trust among participants.

Bugs in the Blockchain's Core Code: Even with thorough testing, there is always a risk that unknown bugs may exist in a blockchain protocol, which could be exploited to disrupt network operations or manipulate account balances. Continuous code review, audit trails, and having a bug bounty program are essential to identify and rectify such vulnerabilities promptly.

Smart Contract Security Risk: Smart contracts are code running on a blockchain, executing the programmed functions automatically if the defined conditions are fulfilled. Bugs or vulnerabilities in smart contract code can expose blockchain networks to potential hacks and exploits. Any flaw in the code can lead to unintended consequences, such as the loss of crypto-assets or unauthorized access to sensitive data.

Dependency on Underlying Technology: Blockchain technology relies on underlying infrastructures, such as specific hardware or network connectivity, which may themselves be vulnerable to attacks, outages, or other interferences.

Risk of Technological Disruption: Technological advancements or the emergence of new technology could impact blockchain systems, or components used in it, by making them insecure or obsolete (e.g. quantum computing breaking encryption paradigms). This could lead to theft or loss of crypto-assets or compromise data integrity on the network.

Governance Risk: Governance in blockchain technology encompasses the mechanisms for making decisions about network changes and protocol upgrades. Faulty governance models can lead to ineffective decision-making, slow responses to issues, and potential network forks, undermining stability and integrity. Moreover, there is a risk of disproportionate influence by a group of stakeholders, leading to centralized power and decisions that may not align with the broader public's interests.

Anonymity and Privacy Risk: The inherent transparency and immutability of blockchain technology can pose risks to user anonymity and privacy. Since all transactions are recorded on a public ledger, there is potential for sensitive data to be exposed. The possibility for the public to link certain transactions to a specific address might expose it to phishing attacks, fraud, or other malicious activities.

Data Corruption: Corruption of blockchain data, whether through software bugs, human error, or malicious tampering, can undermine the reliability and accuracy of the system.

Third-Party Risks: Crypto-assets often rely on third-party services such as exchanges and wallet providers for trading and storage. These platforms can be susceptible to security breaches, operational failures, and regulatory non-compliance, which can lead to the loss or theft of crypto-assets.

I.6 Mitigation Measures

Not applicable.

A. Part A - Information about the person seeking admission to trading

A.1 Name

Ika Foundation

A.2 Legal Form

Not applicable.

A.3 Registered Address

Not applicable.

A.4 Head Office

Not applicable.

A.5 Registration Date

2025-07-17

A.6 Legal Entity Identifier

Not applicable.

A.7 Another Identifier Required Pursuant to Applicable National Law

Not applicable.

A.8 Contact Telephone Number

Not applicable.

A.9 E-mail Address

legal@ika.foundation

A.10 Response Time (Days)

030

A.11 Parent Company

Not applicable.

A.12 Members of the Management Body

Full Name	Business Address	Function
Adam Sax	79 Town Hall Road, West Bay, P.O. Box 1369, George Town, Grand Cayman, Cayman Islands KY1-1108	Executive Director

A.13 Business Activity

The Ika Foundation is a Cayman foundation company, established for the purposes of stewarding the Ika project and supporting its ecosystem. To that end, It enters into agreements with third parties, provides grants and participates in ecosystem development efforts. It has a collaborative relationship with dWallet Labs Ltd., and is managed by professional independent directors.

A.14 Parent Company Business Activity

Not applicable.

A.15 Newly Established

True

A.16 Financial Condition for the past three Years

Not applicable.

A.17 Financial Condition Since Registration

As the person seeking admission to trading of the crypto-asset was only just established, there is no three-year track record of historical financial data. However, the project has garnered interest across institutional investors, with over $21M in funding to date. Overall, the Foundation’s financial condition is healthy, positioning it to fund current and planned activities.

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

B.1 Issuer different from person seeking admission to trading

true

B.2 Name

Name of the issuer (e.g., as shown in the commercial register).

dWallet Labs Ltd.

B.3 Legal Form

Not applicable.

B.4 Registered Address

Not applicable.

B.5 Head Office

Not applicable.

B.6 Registration Date

2022-04-03

B.7 Legal Entity Identifier

Not applicable.

B.8 Another Identifier Required Pursuant to Applicable National Law

516591872

B.9 Parent Company

Not applicable.

B.10 Members of the Management Body

Identity (names or other identifiers), business address and functions of each person that is member of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the issuer.

Full Name	Business Address	Function
Omer Sadika	Har Sinai 2, Tel Aviv, Israel	Director & CEO

B.11 Business Activity

A cybersecurity R&D-focused company, specializing in blockchain technology, and core contributor of Ika

B.12 Parent Company Business Activity

Not applicable.

C. 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 white paper under Article 6 (1) second subparagraph MiCA

Not applicable.

C.14 Reason for drawing up the white paper under Article 6 (1) second subparagraph MiCA

Not applicable.

D. Part D - Information about the crypto-asset project

D.1 Crypto-Asset Project Name

Ika

D.2 Crypto-Assets Name

IKA Token

D.3 Abbreviation

IKA

D.4 Crypto-Asset Project Description

Ika will operate as an MPC network that is coordinated on Sui. Ika will enable zero-trust threshold signatures by using the 2PC-MPC cryptographic scheme, and will achieve resilience and censorship resistance by using a token, the Ika token (IKA), to incentivize network participants to participate in threshold signing & consensus validation and to ensure that there is a provably fair mechanism, a proof-of-stake mechanism, to permissionlessly determine who can become a network participant and how signing power (and thus rewards) is distributed.

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

Full Name	Business Address	Function
Ika Foundation (Cayman Foundation Company)	79 Town Hall Road, West Bay, P.O. Box 1369, George Town, Grand Cayman, Cayman Islands KY1-1108	Ika ecosystem steward
Ika Foundation (Zug)	Gubelstrasse 11, 6300 Zug, Switzerland	Ika ecosystem steward
dWallet Labs Ltd.	2 Har Sinai, Tel Aviv, Israel	Core contributor

D.6 Utility Token Classification

True

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

IKA is the mechanism for paying fees to enable operation of the network, maintaining and securing the network by enabling staking, and ensuring decentralized governance:

Payment - users pay nodes in the MPC network for their work, ensuring a robust economic system. Users pay for operations like generating a new dWallet, requesting signatures to be completed by the network share of a dWallet, and resharing the user and network share of a dWallet.

Security - a reliable network that rewards good actors and punishes adversarial behavior can be enabled by a permissionless delegated proof of stake mechanism for MPC and consensus validation. Users participate in securing the Ika MPC network by staking their IKA tokens.

Governance - Ika's MPC nodes vote on protocol adjustments, and ensure decentralized control over protocol functionality and economics.

D.8 Plans for the Token

In addition to staking, governance, and payment utility, the IKA token also underpins the nuanced economic landscape of cryptographic operations within the Ika network. Different cryptographic functions incur varying computational costs, which in turn influence how users are charged for

interacting with the network. For instance, factors such as different elliptic curves of different cryptographic algorithms like ECDSA, EdDSA, or Schnorr, affect the computational cost of generating a decentralized wallet (dWallet) through Distributed Key Generation (DKG), and the cost of producing threshold signatures. These algorithmic differences are not just theoretical—they translate into tangible cost variations that are reflected in the fees paid by users for different cryptographic operations.

Another key consideration is the cost of maintaining and adapting the MPC node committee, the group responsible for carrying out threshold cryptographic tasks. Changing this committee—a process known as reconfiguration—requires significant cryptographic computation to securely redistribute shares of the network's threshold homomorphic decryption key among the new set of participants. This process is essential to maintain decentralization and adaptability, but it adds to the network's resource demands. Similarly, ongoing optimizations such as pre-signature rounds (which allow the network to prepare cryptographic material in advance to reduce latency) contribute to the overall workload. These behind-the-scenes computations are critical for maintaining the protocol's performance and security, but they must be accounted for in the cost structure borne by users.

To ensure that these costs are handled efficiently and sustainably, Ika employs a dynamic market-driven pricing mechanism using the IKA token. This model is designed to balance incentives across the ecosystem—ensuring that MPC nodes are adequately rewarded for their computational effort and reliability, while keeping pricing competitive and predictable for users. This dynamic equilibrium fosters a self-regulating economy that can adapt to changing demand, cryptographic complexity, and participant behavior. Ultimately, the goal is to achieve a stable, performant network that is both attractive for users and economically sustainable for contributors.

D.9 Resource Allocation

The project received over $20M in funding, including a strategic investment from Sui Foundation.

The project also had a record-setting 1.4M SUI NFT art campaign on Sui, signaling strong community interest.

D.10 Planned Use of Collected Funds or Crypto-Assets

Not applicable.

E. 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

ATTR

E.2 Reasons for Public Offer or Admission to Trading

The Ika Foundation seeks admission of the Token to trading in order to enable more individuals to obtain and use the Token so that they can use, contribute, and participate in the Ika Network. Additionally, by seeking admission to trading, they aim to increase the liquidity of the Token, facilitating equitable access and its exchangeability.

E.3 Fundraising Target

Not applicable.

E.4 Minimum Subscription Goals

Not applicable.

E.5 Maximum Subscription Goal

Not applicable.

E.6 Oversubscription Acceptance

Not applicable.

E.7 Oversubscription Allocation

Not applicable.

E.8 Issue Price

Not applicable.

E.9 Official Currency or Any Other Crypto-Assets Determining the Issue Price

Not applicable.

E.10 Subscription Fee

Not applicable.

E.11 Offer Price Determination Method

Not applicable.

E.12 Total Number of Offered/Traded Crypto-Assets

Not applicable.

E.13 Targeted Holders

ALL

E.14 Holder Restrictions

The purchase of the Token from EU-regulated Exchanges will be available to all users of such Exchanges. Most trading and exchange services offered by Exchanges are open to retail holders, and may be subject to the compliance requirements of the respective Exchange.

The Exchanges may impose restrictions on holders of Tokens on their respective Exchanges, in accordance with applicable laws and internal policies.

E.15 Reimbursement Notice

Not applicable.

E.16 Refund Mechanism

Not applicable.

E.17 Refund Timeline

Not applicable.

E.18 Offer Phases

Not applicable.

E.19 Early Purchase Discount

Not applicable.

E.20 Time-Limited Offer

Not applicable.

E.21 Subscription Period Beginning

Not applicable.

E.22 Subscription Period End

Not applicable.

E.23 Safeguarding Arrangements for Offered Funds/Crypto-Assets

Not applicable.

E.24 Payment Methods for Crypto-Asset Purchase

Not applicable.

E.25 Value Transfer Methods for Reimbursement

Not applicable.

E.26 Right of Withdrawal

Not applicable.

E.27 Transfer of Purchased Crypto-Assets

Not applicable.

E.28 Transfer Time Schedule

Not applicable.

E.29 Purchaser's Technical Requirements

Technical requirements will be specified by the Exchanges and may include the following:

1. A compatible digital wallet or account on supported Exchange;

2. Internet access;

3. A device (computer or mobile) to manage digital wallet/private key and/or account on exchange to carry out transactions

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

Not applicable.

E.31 CASP identifier

Not applicable.

E.32 Placement Form

NTAV

E.33 Trading Platforms name

Trading platforms for which admission to trading is sought include:

- Bitvavo
- Kraken
- OKX
- Binance
- Coinbase
- Bitget
- crypto.com
- Gate.io

E.34 Trading Platforms Market Identifier Code (MIC)

Not applicable.

E.35 Trading Platforms Access

Investors can access trading platforms where IKA tokens are listed by creating an account on the respective platform, completing the required identity verification (KYC) processes, and funding their accounts with supported cryptocurrencies or fiat currencies. Once registered and funded, investors can search for the IKA token trading pair and place buy or sell orders directly through the platform's interface. Detailed guides and tutorials are typically available on the trading platforms to assist investors with navigating and using their services.

E.36 Involved Costs

Trading venues that support IKA establish their own independent fee structures, which may include various charges for transactions, withdrawals, and other services. These fees are set and managed solely by the platforms themselves, with no involvement from the Ika Foundation. Users should carefully review and understand their chosen platform's fee structure before conducting any transactions.

E.37 Offer Expenses

Not applicable.

E.38 Conflicts of Interest

The persons involved in the admission to trading of IKA tokens do not have any conflicts of interest that could materially impact the admission to trading process or its outcome. Should any potential conflicts arise, they will be promptly disclosed and managed in accordance with applicable regulatory requirements and best practices to ensure fair and transparent trading conditions.

E.39 Applicable Law

Laws of England and Wales

E.40 Competent Court

Arbitration as per the rules of the International Chamber of Commerce.

F. Part F - Information about the crypto-assets

F.1 Crypto-Asset Type

The IKA token is classified as an "other crypto-asset" under the Markets in Crypto-Assets Regulation (EU) 2023/1114 (MiCA), as it does not qualify as an asset- referenced token or an e-money token.

F.2 Crypto-Asset Functionality

IKA is the mechanism for paying fees to enable operation of the network, maintaining and securing the network by enabling staking, and ensuring decentralized governance:

Payment - users pay nodes in the MPC network for their work, ensuring a robust economic system. Users pay for operations like generating a new dWallet, requesting signatures to be completed by the network share of a dWallet, and resharing the user and network share of a dWallet.

Security - a reliable network that rewards good actors and punishes adversarial behavior can be enabled by a permissionless delegated proof of stake mechanism for MPC and consensus validation. Users participate in securing the Ika MPC network by staking their IKA tokens.

Governance - Ika's MPC nodes vote on protocol adjustments, and ensure decentralized control over protocol functionality and economics.

F.3 Planned Application of Functionalities

The functionalities described in F.2 above will be in place the moment the mainnet of Ika network goes live, which will take place prior to trading of IKA token being available on any trading platform. However, reference can be made to section D.8 "Plans for the token" for additional details on the IKA's token functionality.

F.4 Type of white paper

OTHR

F.5 The type of submission

NEWT

F.6 Crypto-Asset Characteristics

The IKA token is a crypto-asset as defined by article 3(1)(5) of the Markets in Crypto-Assets Regulation (EU) 2013/1114 ('MiCA').

Symbol: IKA

Initial supply: 10,000,000,000 tokens

Blockchain platform: Sui

Token Standard: Sui Move Coin Standard

F.7 Commercial name or trading name

Ika

F.8 Website of the issuer

https://ika.xyz

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

2025-07-29

F.10 Publication date

2025-07-21

F.11 Any other services provided by the issuer

The Issuer does not provide any other services not covered by Regulation (EU) 2023/1114.

F.12 Identifier of operator of the trading platform

Not applicable.

F.13 Language or languages of the white paper

English.

F.14 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

Not applicable.

F.15 Functionally Fungible Group Digital Token Identifier, where available

Not applicable.

F.16 Voluntary data flag

False.

F.17 Personal data flag

True.

F.18 LEI eligibility

True.

F.19 Home Member State

Malta.

F.20 Host Member States

The admission to trading of the Token is passported in the following countries:

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech
- Germany
- Denmark
- Estonia
- Spain
- Finland
- France

- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Sweden

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

G.1 Purchaser Rights and Obligations

The IKA tokens do not have any inherent rights or obligations attached to them

G.2 Exercise of Rights and Obligation

Not applicable.

G.3 Conditions for Modifications of Rights and Obligations

Not applicable.

G.4 Future Public Offers

Not applicable.

G.5 Issuer Retained Crypto-Assets

Not applicable.

G.6 Utility Token Classification

True

G.7 Key Features of Goods/Services of Utility Tokens

IKA is the mechanism for paying fees to enable operation of the network, maintaining and securing the network by enabling staking, and ensuring decentralized governance:

Payment - users pay nodes in the MPC network for their work, ensuring a robust economic system. Users pay for operations like generating a new dWallet, requesting signatures to be completed by the network share of a dWallet, and resharing the user and network share of a dWallet.

Security - a reliable network that rewards good actors and punishes adversarial behavior can be enabled by a permissionless delegated proof of stake mechanism for MPC and consensus validation. Users participate in securing the Ika MPC network by staking their IKA tokens.

Governance - Ika's MPC nodes vote on protocol adjustments, and ensure decentralized control over protocol functionality and economics.

G.8 Utility Tokens Redemption

IKA tokens can be used to pay for cryptographic operations and/or stake tokens through the Ika smart contracts on the Sui network.

G.9 Non-Trading Request

True

G.10 Crypto-Assets Purchase or Sale Modalities

Not applicable.

G.11 Crypto-Assets Transfer Restrictions

Not applicable.

G.12 Supply Adjustment Protocols

True

G.13 Supply Adjustment Mechanisms

The Ika protocol has inflation, and protocol governance can adjust inflation to be higher or lower or remove it completely.

G.14 Token Value Protection Schemes

False

G.15 Token Value Protection Schemes Description

Not applicable.

G.16 Compensation Schemes

False

G.17 Compensation Schemes Description

Not applicable.

G.18 Applicable Law

Laws of England and Wales

G.19 Competent Court

Arbitration as per the rules of the International Chamber of Commerce.

H. Part H – information on the underlying technology

H.1 Distributed ledger technology

The IKA token will be deployed on the Sui Network, using the Sui Move coin standard.

H.2 Protocols and Technical Standards

The IKA token is a crypto-asset as defined by article 3(1)(5) of the Markets in Crypto-Assets Regulation (EU) 2013/1114 ('MiCA') that utilises the Sui Move Coin standard on the Sui Network. As a Sui token, IKA will follow standardized rules for token transfers, transaction approvals, data access, and supply management, ensuring compatibility with cryptocurrency wallets, exchanges, and DeFi applications. The token will be deployed with an initial supply of 10 billion tokens, and the IKA token can be accessed using any wallet that supports the Sui Network and tokens based on the Sui Move Coin standard.

H.3 Technology Used

Ika's tech stack also includes the Ika Network, an MPC network based on the novel 2PC-MPC cryptographic threshold signature scheme. The Ika Network utilizes a modified version of Mysticeti (Sui's consensus)

H.4 Consensus Mechanism

The Ika Network leverages a dual consensus architecture to meet the distinct requirements of its decentralized orchestration: one for the coordination of digital assets on-chain, and another for high-performance coordination within its cryptographic multiparty computation (MPC) protocol.

Sui Layer – Mysticeti-Based Blockchain Consensus

On the blockchain layer, Ika is coordinated through the Sui network, which uses Mysticeti, a high-performance consensus protocol designed for low latency and high throughput. Unlike traditional leader-based consensus schemes, Mysticeti allows multiple validators to propose blocks concurrently in a DAG (Directed Acyclic Graph) structure, maximizing network bandwidth and improving censorship resistance. This structure permits rapid block propagation and commitment, requiring only three communication rounds—the theoretical minimum—to finalize transactions.

Mysticeti's innovative implicit commitment mechanism reduces the need for extensive vote exchange and certification, thereby cutting down communication overhead and improving bandwidth efficiency. This approach enables average consensus latencies around 0.5 seconds while supporting throughput rates exceeding 200,000 transactions per second in practical settings. In controlled tests, Mysticeti has demonstrated scalability up to 400,000 TPS with latencies remaining under one second on a 50-node network—more than double the throughput of competing protocols.

Because Mysticeti finalizes transactions immediately upon their inclusion in the consensus structure, there's no reliance on subsequent transaction referencing, making it resilient even in low activity or adversarial network conditions. For Ika, this provides a reliable and fast settlement layer for user-initiated operations and control signals.

Ika Network Layer – Mysticeti for MPC Coordination

Internally, Ika employs a parallel instance of Mysticeti within its own network to coordinate between parties in its 2PC-MPC protocol. Here, consensus is not used for asset finality but for secure, ordered, and reliable broadcast of cryptographic inputs across MPC participants.

Given the performance-critical nature of key management and threshold signature generation, Ika benefits from Mysticeti’s low-latency properties to ensure minimal delay in reaching agreement on

secret shares and computation steps. The use of Mysticeti in this off-chain setting ensures that the MPC layer achieves near real-time responsiveness while maintaining robustness against faults and leader unavailability.

Combined Architecture

By integrating Mysticeti both on-chain (via Sui) and off-chain (within Ika's MPC communication stack), Ika achieves end-to-end consensus guarantees optimized for speed, scalability, and fault tolerance. This layered approach ensures that both user-facing transactions and behind-the-scenes cryptographic coordination operate with consistency, performance, and security.

H.5 Incentive Mechanisms and Applicable Fees

The Ika architecture is composed of two interdependent economic layers: the Sui Network, which provides the blockchain coordination layer, and the Ika Network, which powers decentralized key management and policy enforcement via threshold cryptography. Each layer maintains its own incentive structure and fee model, designed to ensure the security, availability, and sustainability of the protocol.

Sui Network: Proof of Stake and Fee Structure

The Sui blockchain, which Ika leverages for asset orchestration, operates under a delegated Proof of Stake (PoS) model. Validators stake SUI tokens to participate in consensus and are rewarded proportionally to their stake and performance. Sui's PoS mechanism promotes economic security by aligning validator incentives with network health.

Transactions on Sui incur fees denominated in SUI, which are used to compensate validators and support ongoing operations. A portion of each fee is deposited into a storage fund, a unique mechanism that subsidizes the long-term cost of storing on-chain data. This fund helps mitigate blockchain bloat by making storage a first-class economic consideration, thereby encouraging developers to manage state efficiently.

For transactions initiated by Ika, such as policy changes or on-chain control actions, users are required to pay SUI-denominated gas fees, which cover the cost of execution and persistence on the Sui ledger.

Ika Network: Node Incentives and IKA-Based Fees

The Ika Network introduces a parallel incentive system to support the distributed set of node operators responsible for executing threshold cryptographic operations (e.g., key generation, signing, and policy enforcement). Like Sui, Ika employs a proof of stake mechanism, where node operators stake IKA tokens to participate in the protocol and to signal their commitment to correct behavior.

Users engaging with the Ika Network pay a separate fee in IKA, which is distributed to the node operators based on their performance and stake. This mechanism ensures the economic sustainability of the off-chain infrastructure and aligns the interests of participants with the operational reliability of the network.

Dual-Fee Model: Coordinating Cross-Layer Operations

When users interact with the Ika protocol—whether for initiating a control transaction, rotating a key, or enforcing an access policy—they incur a dual fee obligation: A SUI fee, paid to the Sui validators, for processing the associated on-chain coordination logic and an IKA fee, paid to the Ika Network node operators, for executing the required off-chain cryptographic operations.

This two-tiered fee system reflects the hybrid nature of Ika's architecture. It ensures that both the blockchain layer (Sui) and the cryptographic coordination layer (Ika) are independently incentivized to operate securely, efficiently, and without reliance on centralized intermediaries.

H.6 Use of Distributed Ledger Technology

False

H.7 DLT Functionality Description

Not applicable.

H.8 Audit

True

H.9 Audit Outcome

Multiple audits have been completed and are continuously being performed by reputable 3rd party audit companies, and are regularly published. Wherever issues are uncovered they are promptly resolved, and there are currently no open and/or unresolved issues identified in any such audit.

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

J.1 Mandatory information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

General information	
S.1 Name *Name reported in field A.1*	Ika Foundation
S.2 Relevant legal entity identifier Identifier referred to in field A.2	Not applicable
S.3 Name of the crypto-asset Name of the crypto-asset, as reported in field D.2	IKA Token
S.4 Consensus Mechanism The consensus mechanism, as reported in field H.4	The Ika Network leverages a dual consensus architecture to meet the distinct requirements of its decentralized orchestration: one for the coordination of digital assets on-chain, and another for high-performance coordination within its cryptographic multiparty computation (MPC) protocol. **Sui Layer – Mysticeti-Based Blockchain Consensus** On the blockchain layer, Ika is coordinated through the Sui network, which uses Mysticeti, a high-performance consensus protocol designed for low latency and high throughput. Unlike traditional leader-based consensus schemes, Mysticeti allows multiple validators to propose blocks concurrently in a DAG (Directed Acyclic Graph) structure, maximizing network bandwidth and improving censorship resistance. This structure permits rapid block propagation and commitment, requiring only three communication rounds—the theoretical minimum—to finalize transactions. Mysticeti's innovative implicit commitment mechanism reduces the need for extensive vote exchange and certification, thereby cutting down communication overhead and improving bandwidth efficiency. This approach enables average consensus latencies around 0.5 seconds while supporting throughput rates exceeding 200,000 transactions per second in practical settings. In controlled tests, Mysticeti has demonstrated scalability up to 400,000 TPS with latencies remaining under one second on a 50-node network—more than double the throughput of competing protocols.

	Because Mysticeti finalizes transactions immediately upon their inclusion in the consensus structure, there's no reliance on subsequent transaction referencing, making it resilient even in low activity or adversarial network conditions. For Ika, this provides a reliable and fast settlement layer for user-initiated operations and control signals. **Ika Network Layer – Mysticeti for MPC Coordination** Internally, Ika employs a parallel instance of Mysticeti within its own network to coordinate between parties in its 2PC-MPC protocol. Here, consensus is not used for asset finality but for secure, ordered, and reliable broadcast of cryptographic inputs across MPC participants. Given the performance-critical nature of key management and threshold signature generation, Ika benefits from Mysticeti's low-latency properties to ensure minimal delay in reaching agreement on secret shares and computation steps. The use of Mysticeti in this off-chain setting ensures that the MPC layer achieves near real-time responsiveness while maintaining robustness against faults and leader unavailability. **Combined Architecture** By integrating Mysticeti both on-chain (via Sui) and off-chain (within Ika's MPC communication stack), Ika achieves end-to-end consensus guarantees optimized for speed, scalability, and fault tolerance. This layered approach ensures that both user-facing transactions and behind-the-scenes cryptographic coordination operate with consistency, performance, and security.
S.5 Incentive Mechanisms and Applicable Fees Incentive mechanisms to secure transactions and any fees applicable, as reported in field H.5	The Ika architecture is composed of two interdependent economic layers: the Sui Network, which provides the blockchain coordination layer, and the Ika Network, which powers decentralized key management and policy enforcement via threshold cryptography. Each layer maintains its own incentive structure and fee model, designed to ensure the security, availability, and sustainability of the protocol. **Sui Network: Proof of Stake and Fee Structure** The Sui blockchain, which Ika leverages for asset orchestration, operates under a delegated Proof of Stake (PoS) model. Validators stake SUI tokens to participate in consensus and are rewarded proportionally to their stake and performance. Sui's PoS mechanism promotes economic security by aligning validator incentives with network health.

	Transactions on Sui incur fees denominated in SUI, which are used to compensate validators and support ongoing operations. A portion of each fee is deposited into a storage fund, a unique mechanism that subsidizes the long-term cost of storing on-chain data. This fund helps mitigate blockchain bloat by making storage a first-class economic consideration, thereby encouraging developers to manage state efficiently. For transactions initiated by Ika, such as policy changes or on-chain control actions, users are required to pay SUI-denominated gas fees, which cover the cost of execution and persistence on the Sui ledger. **Ika Network: Node Incentives and IKA-Based Fees** The Ika Network introduces a parallel incentive system to support the distributed set of node operators responsible for executing threshold cryptographic operations (e.g., key generation, signing, and policy enforcement). Like Sui, Ika employs a proof of stake mechanism, where node operators stake IKA tokens to participate in the protocol and to signal their commitment to correct behavior. Users engaging with the Ika Network pay a separate fee in IKA, which is distributed to the node operators based on their performance and stake. This mechanism ensures the economic sustainability of the off-chain infrastructure and aligns the interests of participants with the operational reliability of the network. **Dual-Fee Model: Coordinating Cross-Layer Operations** When users interact with the Ika protocol—whether for initiating a control transaction, rotating a key, or enforcing an access policy—they incur a dual fee obligation: A SUI fee, paid to the Sui validators, for processing the associated on-chain coordination logic and an IKA fee, paid to the Ika Network node operators, for executing the required off-chain cryptographic operations. This two-tiered fee system reflects the hybrid nature of Ika's architecture. It ensures that both the blockchain layer (Sui) and the cryptographic coordination layer (Ika) are independently incentivized to operate securely, efficiently, and without reliance on centralized intermediaries.
S.6 Beginning of the period to which the disclosure relates	2025-07-17
S.7 End of the period to which the disclosure relates	2025-07-21
Mandatory key indicator on energy consumption	

S.8 Energy consumption Total amount of energy used for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, expressed per calendar year	1,114,713.8
Sources and methodologies	
S.9 Energy consumption sources and Methodologies Sources and methodologies used in relation to the information reported in field S.8	The estimated energy consumption provided in J.08 has been calculated using the CCRI Crypto Sustainability Metrics provided by the Crypto Carbon Ratings Institute (source: https://indices.carbon-ratings.com). Although no credible information exists yet for Ika Network energy consumption, we took the Sui Network figures as reference, although we do estimate Ika Network's energy consumption to be much lower, as both the node count and the hardware requirements for node operators are lower than Sui Network.