ZKsync Association

("Issuer")

White paper pursuant to Title II of Regulation (EU) 2023/1114 ("MiCAR")
in relation to the ZK Token ("Token")

Regulatory Information / Disclaimer

No.	Field	Content Reported
00	Table of Content	
01	Date of notification	2025-09-24
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 Issuer 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 MiCAR 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.

No.	Field	Content Reported
05	Statement in accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114	Not applicable, as the crypto-asset referred to in this white paper does not qualify as a utility token within the meaning of Article 3 para 1 no 9 MiCAR.
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. An offer to the public of this crypto-asset would 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 Token is the native / protocol token of the ZKsync protocol, a permissionless Layer 2 scaling solution for the Ethereum blockchain that aims to leverage zero-knowledge rollups (ZK-rollups) to enable higher-throughput and lower transaction fees compared to the execution of the same transaction directly on Ethereum, while inheriting Ethereum's security. The Token does not confer rights to profits, dividends, or fund distributions. Rather, it exclusively offers its holders the functionality to participate in the on-chain, code-based governance of the ZKsync protocol. This governance function is embedded in a multi governance body system built into the ZKsync protocol itself and controls all changes to the code, and as such the system itself. Through the governance function, Token holders and other governing bodies control system upgrades (both emergency and ordinary course upgrades) or determine governance structures for governing bodies.

No.	Field	Content Reported
		The Token follows the ERC-20 standard, is fungible and freely transferable between users. Individual Token instances are technically and economically fungible, comparable to ETH or other ERC-20 compatible crypto-assets. I.e. aside from transaction history, it makes no difference for the holder which specific Token they hold. Tokens are minted on ZKsync Era (one of the blockchains leveraging ZKsync technology), adhering to a fixed maximum supply of 21,000,000,000 Tokens. Tokens are minted "just-in-time" by smart contracts with capped limits, rather than pre-minting the full supply at once.
09		Not applicable. The crypto-asset referred to in this white paper does not qualify as a utility token within the meaning of Article 3 para 1 no 9 MiCAR.
10	Key information about the offer to the public or admission to trading	Not applicable. The Issuer will not conduct an offer of Tokens to the public within the meaning of Article 3 para 1 no 12 MiCAR or seek admission of the Tokens to trading on a trading platform within the meaning of Article 2 para 2 lit a) in conjunction with Article 3 para 1 no 18 MiCAR with this crypto-asset white paper.

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

Important Notice
The Issuer will not conduct an offer of Tokens to the public within the meaning of Article 3 para 1 no 12 MiCAR or seek admission of the Tokens to trading on a trading platform within the meaning of Article 2 para 2 lit a) in conjunction with Article 3 para 1 no 18 MiCAR with this crypto-asset white paper.

No.	Field	Content Reported
A.1	Name	ZKsync Association - Ein Verein zur Förderung des digitalen Ökosystems ZKsync e.V.
A.2	Legal Form	Association (*Verein*) under Austrian law; ISO standard 20275: DX6Z
A.3	Registered Address	Kärntner Ring 5-7, 1010 Vienna, Austria
A.4	Head office	Kärntner Ring 5-7, 1010 Vienna, Austria
A.5	Registration date	2024-06-14
A.6	Legal entity identifier	529900SV858GPLFCQK64
A.7	Another identifier required pursuant to applicable national law	Austrian Central Register of Associations (*Zentrales Vereinsregister*) register number: 1612209629
A.8	Contact telephone number	Not available. Please see field A.9.
A.9	E-mail address	contact@zknation.io
A.10	Response time (Days)	090 - Meaning the period of days within which the Issuer will reply to inquiries received via the e-mail address listed in field A.9.
A.11	Parent Company	Not applicable. As an Austrian association, the Issuer is an ownerless entity. It does not have shares, stock, equity or any similar instruments. Consequently, the Issuer does not have a parent company.
A.12	Members of the management body	<table><tr><th>Name</th><th>Business address</th><th>Function</th></tr><tr><td>Thomas Bernardini</td><td>Kärntner Ring 5-7, 1010 Vienna, Austria</td><td>Chairman, member of the Issuer's</td></tr></table>

				management board (*Vorstand*)
		Rafael Fernandez	Kärntner Ring 5-7, 1010 Vienna, Austria	Treasurer, member of the Issuer's management board (*Vorstand*)
A.13	Business activity	The activities of the Issuer are not-for-profit. The Issuer therefore has no business activities in the economic sense. Rather, the Issuer's purpose as of the date of this white paper is (collectively, the "**Purpose**"): a) Enhance digital literacy and empower all members of society with the skills and knowledge to understand the blockchain and digital economy with focus on (i) cryptography, especially in the field of zero-knowledge ("**ZK**"), and (ii) blockchain-based networks, systems, architectures, applications and products (collectively, "**Ecosystems**"), particularly those involving ZK and/or artificial intelligence ("**AI**") and promote the development and dissemination of such knowledge, techniques and methods by others; b) Support the development of secure, transparent and censorship resistant digital infrastructures for the benefit of society; c) Ensure access for all members of society to secure, transparent and censorship resistant digital infrastructures; d) Promote the values of freedom, privacy, self-sovereignty, decentralized systems, self-governance and censorship resistance using ZK, blockchain and/or AI technology to ensure the values of a democratic and pluralistic world can be upheld in the digital age for all members of society; e) Promote the democratization and decentralization of blockchain technology and ensure that engagement in the development and governance of ZK protocols and similar technology is possible for all individuals, irrespective of their origin and financial resources; f) Remove financial barriers to entry and foster inclusive participation across all sectors of society in the spirit of a truly decentralized and collaborative digital ecosystem. g) In pursuing the Purpose, the Issuer shall (and in making decisions concerning the Issuer, the Issuer's general assembly and the Issuer's board shall) set aside their direct and indirect personal interests and act solely in furtherance of the best interests of Issuer.		

		As of the date of this white paper, it is intended to achieve the Purpose through the following activities: 1) Develop and disseminate knowledge, techniques and methods for blockchain-based community self-governance systems, particularly with respect to the ZKsync blockchain protocol; 2) Promote and establish a public library of resources, including research papers, educational materials and open-source software, freely accessible to all members of society; 3) Promote the adoption and use of the ZKsync protocol and/or other ZK-enabled blockchains and their Ecosystems by developers, researchers, teachers, students, founders, creators, users and enthusiasts (collectively, the "**ZK Community**"); 4) Support the acquisition and equitable distribution of crypto-assets like the Token via free airdrops and enable the delegation of governance rights to non-token holders; 5) Operate and make publicly available to all members of society (free of charge) a governance portal for at least one zero-knowledge Layer 2 blockchain, which includes a forum for community proposals and discussion, blockchain-based voting tools, governance updates, and related features; 6) Organize and sponsor a range of events (e.g., meetups, hackathons, quests, roundtables, etc.) and maintain electronic channels (e.g., social media communications, message groups, and other online interactions, etc.) to facilitate the exchange of ideas between members of society, ensuring promotion of wider adoption of blockchain technology and ZK protocols and the development of open, decentralized governance, blockchains, ZK technologies and/or related applications; These events will cater to various skill levels and include resources for different stakeholders ensuring access to blockchain education and engagement for all members of society. The Issuer will reach out to universities, schools, public institutions and many other stakeholders to reach a broad audience; 7) Ensure compliance with the Markets in Crypto-Assets Regulation (MiCAR) for activities undertaken by the Issuer in connection with the Token, and any other applicable tokens; 8) Assist all interested and eligible members of society as well as the ZK Community in structuring proposals to access the Token for the benefit and growth of blockchain networks using ZKsync technology. Such proposals may be directed to all members of society, including members of the ZK

		Community for software development and educational or research purposes in the areas of decentralized governance, blockchains, ZK and/or AI technologies; and any uses, purposes, products or services related to the foregoing; and 9) Facilitate transparent communication and coordination across the governance bodies for protocols having decentralized governance structures, including the ZKsync ecosystem. The Issuer commits to fostering an environment of open governance, where decision-making processes are clear and accessible to all members of society. As of the time of publication of this crypto-asset white paper, the Issuer intends to extend its activities to Austria as well as to the rest of the world.
A.14	Parent company business activity	Not applicable. Please see field A.11.
A.15	Newly established	True – Meaning that the Issuer has been established for less than three years.
A.16	Financial condition for the past three years	Not applicable. Please see field A.15.
A.17	Financial condition since registration	As described under field A.13, the Issuer is a not-for-profit organization and, thus, has no business activities in the economic sense. In fact, the Issuer is financed exclusively through donations from third parties. To this end, at point of inception, the Issuer was provided a donation from Matter Labs as well as the ZKsync Foundation (in relation to both, please see field D.5). In addition, the Issuer regularly receives additional donations to implement measures that promote the Purpose (as defined in field A.13). As of the time of publication of this crypto-asset white paper, the Issuer expects that approximately 12 months of operating funding are secured on the basis of these donations.

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

No.	Field	Content Reported
B.1 – B.12	[intentionally left blank]	Part B is not applicable, as Part A was completed and the Issuer (as described in Part A) is also the issuer within the meaning of Article 3 para 1 no 10 MiCAR of the Token.

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 para 1, second subparagraph, of Regulation (EU) 2023/1114

No.	Field	Content Reported
C.1 – C.14	[intentionally left blank]	Part C is not applicable. This white paper is not drawn-up by an operator of a trading platform within the meaning of Article 6 para 1 lit c) of Regulation (EU) 2023/1114 or by such other person drawing up the crypto-asset white paper within the meaning of Article 6 para 1, second subparagraph, of Regulation (EU) 2023/1114.

Part D – Information about the crypto-asset project

No.	Field	Content Reported
D.1	Crypto-asset project name	ZKsync
D.2	Crypto-assets name	ZK Token
D.3	Abbreviation	ZK
D.4	Crypto-asset project description	**ZKsync Protocol and Technologies** The ZKsync protocol is a Layer 2 scaling solution built on Ethereum, designed with the goal to enhance blockchain performance while preserving decentralization, security, and user sovereignty. Invented by Matter Labs, ZKsync aims to leverage zero-knowledge rollups (ZK-rollups) to enable high-throughput, low-cost transactions (both compared to executing the same transactions directly on Ethereum) with cryptographic guarantees of correctness. ZKsync protocol and related technologies enable a network of public and private blockchains, called ZKsync Chains, that share a common proof system based on zero-knowledge proofs. ZKsync Chain operators generate succinct cryptographic proofs that demonstrate the correctness of the system's computation (ZK proof) and submit these proofs for verification on Ethereum. As a result, ZKsync inherits Ethereum's security. This process intends to reduce on-chain computation power and data requirements. One production-ready ZKsync Chain, called ZKsync Era, is managed by Matter Labs and supports smart contracts and Ethereum compatibility, enabling developers to deploy scalable dApps with minimal changes. ZKsync Chains are able to interact with each other via ZKsync Gateway, a shared proof aggregation and interoperability layer designed to connect multiple ZKsync-based chains (rollups, validiums, volitions) in a trustless and efficient manner. **ZKsync Governance and Token Utility** The Tokens are ZKsync's protocol token, and are used for ZKsync Governance. Additional Token functionalities may be introduced via ZKsync protocol upgrades as approved and executed via the ZKsync Governance Procedures available at docs.zknation.io (last accessed on: 2025-09-24) - please see also field F.2. The maximum total supply of the Tokens is 21,000,000,000. For more information on the tokenomics / distribution of the Tokens please see field D.9.

<table>
<tr><th>No.</th><th>Field</th><th>Content Reported</th></tr>
<tr><td></td><td></td><td>For the involved persons in relation to the ZKsync protocol and the Tokens please refer to field D.5.</td></tr>
<tr><td>D.5</td><td>Details of all natural or legal persons involved in the implementation of the crypto-asset project</td><td>
ZKsync Association - Issuer
<table>
<tr><th>Name</th><th>Business address / domicile</th><th>Function</th></tr>
<tr><td>ZKsync Association</td><td>Kärntner Ring 5-7, 1010 Vienna, Austria</td><td>See field A.13</td></tr>
</table>
Other legal persons participating in governance procedures
<table>
<tr><th>Name</th><th>Business address / domicile</th><th>Function</th></tr>
<tr><td>ZKsync Security Council Foundation</td><td>103 South Church Street, George Town, Grand Cayman KY1-1106, Cayman Islands</td><td>ZKsync Governance, Emergency Response</td></tr>
<tr><td>ZKsync Guardians Foundation</td><td>103 South Church Street, George Town, Grand Cayman KY1-1106, Cayman Islands</td><td>ZKsync Governance, Emergency Response</td></tr>
<tr><td>ZKsync Foundation</td><td>103 South Church Street, George Town, Grand Cayman KY1-1106, Cayman Islands</td><td>Emergency Response</td></tr>
</table>
Other legal persons involved in the implementation of the crypto-asset project
<table>
<tr><th>Name</th><th>Business address / domicile</th><th>Function</th></tr>
<tr><td>Matter Labs</td><td>122 Mary Street, George Town, Grand Cayman KY1-1206, Cayman Islands</td><td>Engineering</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>No.</th><th>Field</th><th>Content Reported</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Scopelift</td><td>18 Campus Blvd. Ste. 100 Newtown Square, PA 19073</td><td>Engineering</td></tr>
<tr><td>Tally</td><td>234 MacDonough St. Brooklyn, NY 11233</td><td>Engineering</td></tr>
</table>
</td></tr>
<tr><td>D.6</td><td>Utility Token Classification</td><td>False – Meaning that in the view of the Issuer, the Token is not to be qualified as a "utility token" within the meaning of Art 3 para 1 no 9 MiCAR.</td></tr>
<tr><td>D.7</td><td>Key Features of Goods/Services for Utility Token Projects</td><td>Not applicable. Please see field D.6.</td></tr>
<tr><td>D.8</td><td>Plans for the token</td><td>Important Milestones Achieved:

Q1 2019 (zkRollups): Matter Labs announces zkRollups as a generalizable scaling solution for Ethereum.

Q2 2020 (Lite launch): ZKsync 1.0 (later called ZKsync Lite) went live on June 18, 2020 as a ZK-rollup optimized for payments, swaps and NFT minting on Ethereum.

Q4 2022 (ZKsync Era closed mainnet): After a closed testnet in December 2021, ZKsync Era (zkEVM) entered closed mainnet launch in October 2022.

Q1 2023 (ZKsync Era public developer launch): ZKsync Era opened to developers, enabling permissionless contract deployment.

Q3 2023 (Boojum proof system): ZKsync Era rolls out the Boojum STARK-based proof system, designed for GPU-based proving with only 16 GB RAM for prover decentralization.

Q1 2024 (Prover Network first steps): ZKsync began a technical research program focused on decentralizing the proof system, partnering with external teams for design discussions, and to provide APIs for them to integrate provers.

Q2 2024 (Token launch): On June 17, 2024, the Token was launched by the Issuer and the Token Assembly was formed. At launch, multiple minting contracts were deployed for permissionless claiming. These minting contracts allow for the creation of a total of 21 billion tokens. The Token airdrop was live from ~June 17, 2024 through the January 3, 2025 claim deadline.

Q3 2024 (Governance launch): On September 12, 2024, the ZKsync Governance System was activated, supported by the ZKsync Security Council and ZKsync Guardians.</td></tr>
</table>

No.	Field	Content Reported
		Q1 2025 (Decentralized Prover Pilot): ZKsync launches the pilot phase of its Decentralized Prover Network, inviting community members to run provers, submit validity proofs, and earn testnet rewards—laying the groundwork for full-scale, trustless proving. Q2 2025 (EVM Interpreter live): Protocol upgrade v27 delivers EVM (Ethereum Virtual Machine) bytecode compatibility via the EVM Interpreter. The EVM emulator is activated on ZKsync Era mainnet on May 5, 2025. Q2 2025 (Private ZKsync Chains launched): ZKsync enables enterprise-grade private validium chains infrastructure. Q2 2025 (Gateway activation): ZKsync Gateway is live by June 2025 as a proof-aggregation and cross-chain messaging layer for ZKsync Chains, custom blockchains powered by zk-technology and the ZKsync protocol. Q2 2025 (Airbender announced): Matter Labs, the inventor of ZKsync, announces a potential new proof system for ZKsync known as "Airbender" — the open-source RISC-V zkVM delivering ~35 second Ethereum block proofs on a single GPU at the time of announcement. The future plans for the ZKsync network and the Token, as of the date of this crypto-asset white paper, include the following key milestones: ● Activation of Airbender, subject to a successful ZKsync governance vote . ● Implementation of decentralized sequencing supporting Gateway and ZKsync Era, allowing anyone to participate in ZKsync as a sequencer. ● Enabling protocol-level interoperability between ZK Chains. ● Enabling protocol-level fees from the sequencers, such that all ZK Chains are contributing towards the sustainability of the ecosystem.
D.9	Resource Allocation	At launch of the Token in June 2024, multiple minting contracts were deployed, allowing for the creation of up to a total of 21,000,000,000 Tokens. Tokens are minted "just-in-time", with certain allocations designed to support protocol sustainability and ecosystem expansion as follows: ● **Token Airdrop**: ~3.7 billion Token (17.50%) were distributed to approximately 695,000 wallets during the launch period from June 17, 2024 through January 3, 2025, recognizing early users, developers, and contributors across ZKsync Lite and Era. ● **Ecosystem Initiatives and Growth**: ~4.2 billion Token (19.9%) were allocated to the (at launch of the Token

No.	Field	Content Reported
		newly-established) ZKsync Foundation, an independent organisation created to accelerate the adoption of the ZKsync technology. • **Token Assembly**: ~6.4 billion unminted Tokens (~29.3%) remained in control of ZKsync Governance to support protocol sustainability and ecosystem development. • **Protocol Development Team Members and Investors**: ~7.0 billion Tokens (~33.3%) were allocated to team members and investors, compensating the initial builders and supporting previous R&D efforts, infrastructure development, and maintenance of ZKsync Era and Lite. These allocations are subject to industry standard vesting and lock-up schedules such as 1-year cliff followed by a 3 year linear vesting. Allocations to natural and legal persons as part of the launch of the Token are intended to fund the continued open-source development of the network, support the growth of the ecosystem, and cover operational expenses. However, no recipient of Tokens is under any obligation to use them for the benefit of the ZKsync protocol, and any such use is at their sole discretion. All allocations are governed under the oversight of the ZKsync Governance Procedures (see G.3 Conditions for modifications of rights and obligations). Future distributions will be informed by network needs and community deliberation.
D.10	Planned Use of Collected Funds or Crypto-Assets	Not applicable. As the Issuer will not conduct an offer of Tokens to the public within the meaning of Article 3 para 1 no 12 MiCAR with this crypto-asset white paper (please see also field 10 and Part E), the Issuer will not collect any funds or crypto-assets.

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

No.	Field	Content Reported
E.1 – E.40	[intentionally left blank]	Part E is not applicable. The Issuer will neither conduct an offer of Tokens to the public within the meaning of Article 3 para 1 no 12 MiCAR nor seek admission of the Tokens to trading on a trading platform within the meaning of Article 2 para 2 lit a) in conjunction with Article 3 para 1 no 18 MiCAR with this crypto-asset white paper.

Part F – Information about the crypto-assets

No.	Field	Content Reported
F.1	Crypto-Asset Type	The Token is classified as a "crypto-asset" under Article 3 para 1 no 5 MiCAR, falling within the residual category of "other crypto-assets"; i.e. it does not meet the criteria for an asset-referenced token (ART) under Article 3 para 1 no 6 MiCAR, as it does not purport to maintain a stable value by referencing another asset or currency, or the criteria for an electronic money token (EMT) under Article 3 para 1 no 7 MiCAR, as it is not primarily intended as a means of payment linked to a single official currency. The Token does not qualify as a utility token pursuant to Article 3 para 1 no 9 MiCAR.
F.2	Crypto-Asset Functionality	The Token allows holders to participate in the on-chain, code-based governance of the ZKsync protocol. This governance function is built into the ZKsync protocol itself and controls all changes to the code, and as such the system itself. The governance function of the Token requires consensus across three governing bodies: the Security Council, Guardians, and the Token Assembly. The Security Council includes 12 members who are technical security experts in blockchain technologies. Guardians include 8 members who are industry leaders and can veto malicious proposals. The Token Assembly includes token holders who delegate voting power to ZKsync Delegates. ZKsync Delegates vote on governance proposals. Token holders can delegate their voting power, which is 1 vote per Token, via the token contract or the ZKsync Governance Portal available at delegate.zknation.io. Through the governance function, Token holders and other governing bodies control system upgrades (both emergency and ordinary course upgrades) and determine governance structures for governing bodies as described in the ZKsync Governance Procedures available under https://docs.zknation.io/zksync-governance-procedures/zksync-governance-procedures-overview (last accessed on: 2025-09-24).
F.3	Planned Application of Functionalities	See F.2 – All crypto-asset functionalities were deployed at launch. Additional Token functionalities may be introduced via Zksync protocol upgrades as approved and executed from time to time via the Governance Procedures.

No.	Field	Content Reported
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 white paper	OTHR – meaning that this crypto-asset white paper concerns crypto-assets other than asset-referenced tokens and e-money tokens.
F.5	The type of submission	NEWT – meaning that this is a new submission of a crypto-asset white paper.
F.6	Crypto-Asset Characteristics	The characteristics of the Token are: 1. **Token standard:** ERC-20 2. **Underlying blockchain**: Ethereum (L1), ZKsync Era (L2) 3. **Transferability**: Tokens are freely transferable between users. Individual token instances are technically and economically fungible, comparable to ETH or other ERC-20 compatible crypto-assets. I.e. aside from transaction history, it makes no difference for the holder which specific Token they hold. 4. **Token supply:** Fixed at 21 billion Tokens, to be minted and claimed on demand by approved (minting eligible) addresses. Currently, no rolling minting/burning mechanisms are established.
F.7	Commercial name or trading name	Not applicable, as a DTI is provided in F.13.
F.8	Website of the issuer	zknation.io
F.9	Starting date of offer to the public or admission to trading	Not applicable. The Issuer will not conduct an offer of the crypto—asset referred to in this white paper (i.e. the Tokens) to the public within the meaning of Article 3 para 1 no 12 MiCAR or seek admission to trading of the Tokens on a trading platform within the meaning of Article 2 para 2 lit (a) in conjunction with Art 3 para 1 no 18 MiCAR with this crypto-asset white paper. Please see part E.
F.10	Publication date	2025-10-22
F.11	Any other services provided by the issuer	Not applicable.
F.12	Language or languages of the white paper	This crypto-asset white paper is drafted solely in English.

No.	Field	Content Reported
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	HKL2NKLD8
F.14	Functionally Fungible Group Digital Token Identifier, where available	BCBLPFRBX
F.15	Voluntary data flag	True – meaning that this crypto-asset white paper is drawn up voluntarily. The Issuer will not conduct an offer of the crypto—asset referred to in this white paper (i.e. the Tokens) to the public within the meaning of Article 3 para 1 no 12 MiCAR or seek admission to trading of the Tokens on a trading platform within the meaning of Article 2 para 2 lit (a) in conjunction with Art 3 para 1 no 18 MiCAR with this crypto-asset white paper. Please see part E.
F.16	Personal data flag	True
F.17	LEI eligibility	True, meaning the Issuer is eligible for a Legal Entity Identifier. Please see field A.6.
F.18	Home Member State	Austria – meaning that Austria is the country in which the Issuer (i.e. the person responsible for drawing up this crypto-asset white paper) is registered.
F.19	Host member state as defined in Article 3 paragraph 34 of Regulation (EU) 2023/1114	Not applicable. Neither will the crypto—asset referred to in this white paper (i.e. the Tokens) be offered to the public nor will an application for admission to trading of the crypto-asset on a trading platform be made under this crypto-asset white paper.

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

No.	Field	Content Reported
G.1	Purchaser Rights and Obligations	The Token does not convey any financial or other rights against the Issuer or any affiliate of the Issuer. There is also no redemption right or claim against the Issuer or any affiliate of the Issuer attached to the Token. The Token does not convey any ownership rights over the ZKsync protocol or any other assets except for ownership of the Token itself and is not used for any distribution of funds or dividend-like distributions of Tokens. On the other hand, holding Tokens does not entail any obligations towards the Issuer or any affiliate of the Issuer. However, obligations may exist towards third parties not affiliated with the Issuer (e.g. tax authorities). While it is not a right against the Issuer, holders of the Token can generally make use of the Token's functionalities on the Zksync protocol as described under fields F.2 and F.3. The Issuer does not guarantee that these functionalities will be available indefinitely. Such functionalities can be modified by a governance proposal that is successfully passed under the Governance Procedures as described under field F.2.
G.2	Exercise of Rights and obligations	Not applicable. Please see field G.1.
G.3	Conditions for modifications of rights and obligations	Not applicable. Please see field G.1.
G.4	Future Public Offers	At the time of publication of this crypto-asset white paper, the Issuer does not have any specific plans to conduct one or more offer(s) of the Token to the public within the meaning of Article 3 para 1 no 21 MiCAR in the future.
G.5	Issuer Retained Crypto-Assets	A total of 200,000 Tokens were retained by the Issuer via a minting contract deployed at launch. All were still available to the Issuer on the date of this crypto-asset white paper.
G.6	Utility Token Classification	False – meaning that this crypto-asset white paper does not concern "utility tokens" within the meaning of Article 3 para 1 no 9 MiCAR.
G.7	Key Features of Goods/Services of Utility Tokens	Not applicable. Please see field G.6.

No.	Field	Content Reported
G.8	Utility Tokens Redemption	Not applicable. Please see field G.6.
G.9	Non-Trading request	False – meaning that admission to trading of the Tokens on a trading platform is not sought in the context / in connection with this crypto-asset white paper. Please see also part E.
G.10	Crypto-Assets purchase or sale modalities	Not applicable. The Issuer will not conduct an offer of the crypto—asset referred to in this white paper (i.e. the Tokens) to the public within the meaning of Article 3 para 1 no 12 MiCAR or seek admission to trading of the Tokens on a trading platform within the meaning of Article 2 para 2 lit (a) in conjunction with Art 3 para 1 no 18 MiCAR with this crypto-asset white paper. Please see part E.
G.11	Crypto-Assets Transfer Restrictions	There are no transfer restrictions associated with the Token. Please also see field F.6.
G.12	Supply Adjustment Protocols	False – meaning that the Token does not have protocols for the increase or decrease of the supply.
G.13	Supply Adjustment Mechanisms	Not applicable. Please see field G.12.
G.14	Token Value Protection Schemes	False - meaning that the Token does not have a protection scheme guaranteeing its value.
G.15	Token Value Protection Schemes Description	Not applicable. Please see field G.14.
G.16	Compensation Schemes	False – meaning that the Token is not subject to a compensation scheme.
G.17	Compensation Schemes Description	Not applicable. Please see field G.16.
G.18	Applicable law	Austrian law (unless otherwise governed by applicable international private law).
G.19	Competent court	Subject to mandatory applicable law, the court in Vienna, Austria, with subject matter jurisdiction shall have exclusive jurisdiction for any and all disputes against the Issuer arising out of or in connection with this crypto-asset white paper.

Part H – Information on the underlying technology

No.	Field	Content Reported
H.1	Distributed ledger technology	Not applicable as a DTI is provided in field F.13.
H.2	Protocols and technical standards	**Ethereum Compatibility** ZKsync Chains are compatible with the Ethereum Virtual Machine (EVM), meaning ZKsync has Solidity based smart contracts, EVM token standards such as ERC20, EVM developer tooling, and standard user wallets. **Cryptography** ZKsync Chains are designed to be flexible to allow a variety of cryptographic options. Users typically sign transactions with ECDSA signatures over either the secp256k1 or secp256r1 curves. Hash functions include SHA256 and Keccak. ZKsync's ZK proof system "Boojum" is designed to prove the Era Virtual Machine (EraVM), which is the system that is source code compatible with the EVM. The unique innovation is the use of "List Polynomial Commitments", detailed in the Redshift paper, published by researchers in the International Association for Cryptologic Research Journal (available at https://eprint.iacr.org/2019/1400.pdf; last accessed on: 2025-09-24). **Open Source** Zksync's code is open sourced under MIT and Apache 2.0 licenses. The codebase is public and actively maintained on Github, allowing for open contributions, transparency, and security.
H.3	Technology Used	**Native Account Abstraction Implementation** Typical blockchain accounts controlled by users are called Externally Owned Accounts ("**EOA**"). It is also possible to have accounts controlled by a smart contract; these are called Smart Accounts. Many blockchains including Ethereum give the option to use one or the other but not both at the same time. ZKsync protocol is special in that all accounts, even EOAs, behave like smart contract accounts; this is called Native Account Abstraction ("**Native AA**"). Zksync's Native AA adheres to many industry standards including EIP-4337 but with a unified mempool for both EOA and Smart Account transactions. **Paymaster Architecture** Paymasters are smart contracts that can pay gas fees in the designed base token as selected by the ZKsync Chain, with arbitrary payment logic including deducting ERC20 tokens from

No.	Field	Content Reported
		users, performing additional checks, or sponsoring transactions without requiring anything in return. **Transaction Types** ZKsync supports legacy, EIP-2930, EIP-1559, and EIP-712 transaction types. EIP-712 transactions are designated with transaction_type 113 and require signing a typed EIP-712 structure instead of RLP-encoded transaction. **Virtual Machine Architecture** EraVM is an EVM-compatible virtual machine built for ZKsync Chains. It was built to be very similar to the Ethereum Virtual Machine while also being easier to ZK prove. EraVM supports Solidity smart contracts, Ethereum signatures, and other common Ethereum functionality. The most observable difference from EVM is the address derivation rule, but ZKsync developers who prefer to use exactly the same CREATE or CREATE2 as Ethereum can use ZKsync's EVM Interpreter. The cost for operations on Era VM differs from EVM. Gas costs are designed to cover operator spends on generating proofs and Ethereum related costs for proof verification & data submission. **EVM Interpreter Layer** The EVM Interpreter allows standard EVM bytecode deployment and execution on top of EraVM. When an EVM contract is deployed, it is tagged with a special identifier and routed through the interpreter, which translates EVM instructions into EraVM operations in real-time. The interpreter targets the Cancun EVM version and enables standard Ethereum tooling compatibility. Key Limitations: ● No delegate call between EVM and EraVM contracts ● Higher gas costs than native EraVM bytecode ● CALLCODE, SELFDESTRUCT, BLOBHASH, BLOBBASEFEE opcodes not supported ● modexp, blake2f, pointEvaluation precompiles unavailable **STARK-Based Architecture** ZKsync's Boojum Proof System is a STARK-based proof system used to prove ZKsync Chains. Boojum's cryptography includes PLONK-ish arithmetization for transforming general computation into mathematical form, PLONK-ish proof arguments, and FRI commitments. Boojum is based on the

No.	Field	Content Reported
		Redshift cryptography paper (available at https://eprint.iacr.org/2019/1400.pdf; last accessed on: 2025-09-24) which innovated List Polynomial Commitments. **Proof Generation Process** The proving process involves witness generation (creating proof of transaction validity without revealing details), circuit conversion (organizing code into various circuits within virtual machine), and proof system processing through multiples layers of recursion. Proofs are typically split into many pieces for parallelization, and the recursion steps will combine the earlier proofs into a smaller number of proofs, repeatedly until only one proof remains. The last round of proof recursion uses a FFLONK proof to lower costs when posting to Ethereum. **Data Availability and State Management** ZKsync posts "state diffs" to L1 (Ethereum) instead of raw transaction data. State diffs represent changes in blockchain state, with compressed format using enumeration indexes for repeated writes and (derived_key, final_value) pairs for initial writes. Each storage key receives a permanently assigned ID, with enumeration indexes assigned in sorted order of (address, key). **Compression Algorithm** For initial writes: (derived_key, final_value) pairs. For repeated writes: (enumeration_index, final_value) pairs where enumeration_index is at most 8 bytes vs 32 bytes for derived keys (DK), providing significant data compression. **Pubdata Structure** Total pubdata contains: L2→L1 user logs concatenation, 4-byte count of long L2→L1 messages, L2→L1 messages in <4 byte length || actual_message> format, 4-byte count of uncompressed bytecodes, 4-byte length of compressed state diffs, and compressed state diffs. **Message Passing Architecture** ZKsync supports general message passing for L1<->L2 communication. L1->L2 messages are recorded in a priority queue on L1, with the sequencer executing them on L2. For each priority operation, hash and status are sent via L2→L1 log, enabling L1 reconstruction of rolling hash for batch verification. **Priority Operations** Priority operations can be created by any user via the requestL2Transaction method on L1, which performs checks

No.	Field	Content Reported
		ensuring processability and adequate fee compensation. Upgrade transactions can only be created during system upgrades when DiamondProxy performs delegatecall to upgrader implementation. **Bridge Implementation** Bridging uses two communicating contracts (L1 and L2) via L1<->L2 interoperability. For deposits: users call deposit on L1 bridge, tokens are locked, L1 bridge initiates L2 transaction, tokens are minted on L2. For withdrawals: L2 tokens burned, L2->L1 message sent, finalizeWithdrawal called on L1 to unlock funds. **Shared Bridge and Interoperability** SharedBridge stores all funds on L1 and maintains balance of all tokens including ETH supply. It contains mapping from chainId to L2SharedBridge address, looking up the correct L2 bridge for deposits to specific chains. **Multi-Chain Coordination** ZKsync Chains operate with a shared bridge contract on L1 and native bridges between individual rollups. All ZKsync Chains must follow common standards: same empty starting state, identical VM implementations and proof systems, and coordinated upgrade mechanisms. **Ethereum Settlement and Security Model** ZKsync Chains are built on top of smart contracts on Ethereum. Everything that happens on ZKsync Chains will be checked by Ethereum via ZK proofs. In this way, ZKsync Chains obtain many of Ethereum's security properties. In detail, ZKsync Chains will commit, prove, and execute every block. Committing means posting the ZKsync block data to Ethereum (Note: ZKsync actually posts State Diffs of the block data). Proving means submitting a proof that the block was executed correctly. At this point Ethereum knows the block and a proof that it was executed correctly, so it is safe to call "execute" which updates the smart contract on Ethereum to remember the ZKsync Chain's new state. At this point, the ZKsync Chain has "settled" to Ethereum and funds may move directly back to Ethereum. **Gateway and Proof Aggregation** ZKsync's Gateway serves as a communication hub for ZKsync Chains, enabling fast interop through quick proof generation/verification and cost reduction via aggregated proof settlement. Transaction flow involves chains posting their

No.	Field	Content Reported
		proofs to Gateway, Gateway sharing those proofs to other chains, and everything settling together on Ethereum. **Performance Metrics** Current throughput: 100+ TPS on sequencer. Internal benchmarks have reached 10,000 TPS at $0.0001 per transaction for upcoming upgrades. Boojum upgrade decreased Ethereum bytes needed per ZKsync Era transaction from 211 to 68, which means lower costs because more ZKsync transactions can fit in each Ethereum blob compared to non-ZKsync Chains. **ERC20 and Token Standards** ZKsync Stack supports using ERC20 tokens as base tokens for chain fees instead of ETH, enabling chains to use tokens like USDC or custom community tokens as base currency. Base tokens are managed at L2BaseToken system contract with behavior identical to ether on EVM.
H.4	Consensus Mechanism	ZKsync supports customizable architecture that can adapt to different consensus requirements depending on whether a ZKsync Chain wants to run one node or multiple nodes. ZKsync Chains can begin with one sequencer for maximum speed and simplicity, then transition to multiple nodes with the ChonkyBFT consensus algorithm, detailed below, as their needs evolve. Additional details of the ChonkyBFT consensus algorithm are available at: https://arxiv.org/pdf/2503.15380 (last accessed on: 2025-09-24). Regardless of whether a ZKsync chain uses a single sequencer or ChonkyBFT consensus, all chains fundamentally rely on zero-knowledge proofs as their primary security mechanism. This represents a fundamental departure from traditional blockchain architectures that depend on economic incentives and validator honesty. The zero-knowledge proof system, currently called Boojum, creates mathematical proofs that demonstrate the correct execution of all transactions. These proofs are generated after blocks are created and serve as cryptographic evidence that all state transitions were computed correctly according to the network's rules. The proofs are then verified on Ethereum by smart contracts, which either accept or reject them based purely on mathematical validity. Additional details regarding the Boojum proof system are available here: https://github.com/matter-labs/zksync-crypto/blob/main/crates/boojum/README.md (last accessed on: 2025-09-24). This approach means that ZKsync's security doesn't depend on trusting sequencers or validators to behave honestly. Instead, it

No.	Field	Content Reported
		relies on mathematical formulae certainty. Any attempt to create invalid transactions or incorrect state changes will result in proof generation failure or verification rejection on Ethereum. The proof system constrains all participants in the network, whether they are operating as single sequencers or participating in ChonkyBFT consensus. They cannot circumvent the mathematical requirements imposed by the zero-knowledge circuits, which replicate Ethereum Virtual Machine behavior and ensure all operations follow established rules.
H.5	Incentive Mechanisms and Applicable Fees	On Ethereum, transaction security is driven by gas fees, which users pay to compensate miners for validating transactions. Users may set a gas limit and gas price for each transaction individually. The gas limit is the maximum work the transaction can require while the gas price is the amount of ETH the user is willing to pay per unit of gas. Higher gas prices incentivise miners to prioritise those transactions. ZKsync's fee model has been designed to be similar to that of Ethereum, but there is currently no mechanism to have transactions be prioritised. The sequencers process the transactions in the order in which they were submitted. Transaction fees on ZKsync Chains can be paid in ETH or another ERC20 and cover computation, proof generation, and data availability costs. Transaction fees on ZKsync Era, the ZKsync Chain where the ZK token contract is deployed, are paid in ETH. The system amortizes zero-knowledge proof generation across multiple transactions in each batch. Fee levels fluctuate based on network demand and proof generation costs. Fee revenue is distributed to network operators including sequencers and provers who maintain network functionality. Sequencers earn fees for transaction ordering and batch creation, while provers (when the system is decentralized) receive compensation for generating zero-knowledge proofs that validate state transitions. The fees are only distributed upon submission of valid transactions based on the proof system. This economic model incentivizes secure network participation and ensures reliable operation without requiring additional token inflation. The fee structure also serves as a natural spam protection mechanism, preventing network congestion while maintaining accessibility for legitimate users.
H.6	Use of Distributed Ledger Technology	False
H.7	DLT Functionality Description	Not Applicable

No.	Field	Content Reported
H.8	Audit	True
H.9	Audit outcome	Audits have covered core components of the ZKsync system, including the smart contracts deployed on Ethereum mainnet, the zero-knowledge circuits used to generate validity proofs, the cryptographic primitives underpinning transaction security, and the infrastructure supporting data availability and user interaction. These evaluations typically focus on key dimensions such as protocol security, scalability, fault tolerance, operational efficiency, and resistance to known classes of attack. Across all audits conducted to date, any vulnerabilities or potential risks identified have been addressed prior to production deployment. To the best knowledge of the Issuer, all known findings have been acknowledged and resolved. A comprehensive list of audits and their outcomes are available at: https://docs.zksync.io/zksync-protocol/security/audits (last accessed on: 2025-09-24) and include: SSO Account OIDC Recovery Solidity Audit, OpenZeppelin, April 2025. ZKsync Protocol Security Review, Spearbit, April 2025. SSO Account Recovery Circuits Audit, OpenZeppelin, March 2025. EVM Interpreter & Nonces Update Audit, OpenZeppelin, March 2025. Guardian Recovery & Validator Audit, OpenZeppelin, March 2025. Crypto Precompile Audit, OpenZeppelin, March 2025. Era Contracts Precompile Audit, OpenZeppelin, March 2025. Protocol Precompiles Implementation Audit, OpenZeppelin, March 2025. ZKsync Era public contest, CodeHawks, from 2024-10-28 to 2024-12-02. Layer 1 Governance Diff Audit, OpenZeppelin, from 2024-06-05 to 2024-06-12. Protocol Defense Audit, OpenZeppelin, June 2024. Distributor Diff Audit, OpenZeppelin, May 2024. L2 Governance Audit, OpenZeppelin, May 2024. zk-Stack VM 1.5 Diff Audit, OpenZeppelin, April 2024. Paymaster Audit, OpenZeppelin, April 2024.

No.	Field	Content Reported
		Decentralized Governance Audit, OpenZeppelin, from 2024-04-05 to 2024-04-26. ZKsync Audit public contest, Code4rena, March 2024. ZK-Token Capped-Minter & Merkle-Distributor Audit, OpenZeppelin, March 2024. State Transition Diff Audit, OpenZeppelin, March 2024. EIP-4844 Support Audit, OpenZeppelin, February 2024. ZKsync Shared Bridge (USDC) Audit, Audittens, December 2024. ZKsync Gateway Audit, Audittens, September 2024. Short-Term Fee Model Changes, OpenZeppelin, from 2023-12-06 to 2023-12-13. Diff and Governance Audit, OpenZeppelin, from 2023-12-04 to 2023-12-22. Layer 1 & 2 Diff Audit, OpenZeppelin, from 2023-11-27 to 2023-12-05. SNARK Wrapper Audit, Spearbit, November 2023. Layer 1 Messenger Upgrade, OpenZeppelin, from 2023-08-30 to 2023-09-14. Layer 2 Block Refactor, OpenZeppelin, from 2023-07-25 to 2023-07-31. Smart Contract Security Assessment, Halborn, from 2023-07-12 to 2023-07-20. GnosisSafeZk Assessment, OpenZeppelin, from 2023-05-22 to 2023-05-26. Bridge and .transfer & .send, OpenZeppelin, from 2023-04-24 to 2023-05-01. WETH Bridge Audit, OpenZeppelin, from 2023-03-27 to 2023-03-31. Layer 2 System Contracts Public Contest, Code4rena, from 2023-03-10 to 2023-03-19. Layer 2 Fee Model and Token Bridge, OpenZeppelin, from 2023-01-23 to 2023-02-17. ZK Proof System, Halborn, from 2023-01-09 to 2023-03-08. Layer 1 Diff Audit (Upgrade Audit), OpenZeppelin, from 2023-02-06 to 2023-02-17. Layer 2 Bootloader, OpenZeppelin, from 2022-11-28 to 2022-12-23. Layer 1 Diff Audit (Upgrade Audit), OpenZeppelin, from 2022-11-21 to 2022-11-25.

No.	Field	Content Reported
		Layer 1 Public Contest, Code4rena, from 2022-10-28 to 2022-11-09. Layer 2, Matter Labs, from 2022-08-17 to 2022-10-24. Layer 1 Smart Contracts, OpenZeppelin, from 2022-09-05 to 2022-09-30. Layer 1 Smart Contracts, Matter Labs, from 2022-06-14 to 2022-08-17. ZK Proof System, Matter Labs, from 2022-10-24 to 2022-11-18.

Part I – Information on risks

No.	Field	Content Reported
I.1	Offer-Related Risks	Not applicable. The crypto—asset referred to in this white paper (i.e. the Tokens) will not be offered to the public under this crypto-asset white paper. Please see part E.
I.2	Issuer-Related Risks	**Risk of Insolvency**: While the Token does not convey any claims, collateral nor entitles the holder to segregation of assets from the Issuer, in a hypothetical insolvency, Token holders would not have special priority rights. Further, an Issuer insolvency could lead to limitation or cessation of third-party service providers supporting governance activities, e.g. running of the governance portal or code repository (Github) resulting in limited accessibility. **Business Risk**: Issuer relies on ongoing donations primarily from ZKsync ecosystem participants. Should insufficient donations be provided, then operations might be impaired or lead to insolvency of the Issuer. **Operational Risk**: Inadequate or failed internal processes, systems, human error, or cyber incidents, including smart contract vulnerabilities and blockchain network disruptions may lead to reputational damage and/or insolvency of the Issuer. **Credit and Counterparty Risk**: Third-parties holding Issuer's assets (such as exchanges, custodians, etc) could default or fail to meet their obligations vis-a-vis the Issuer. Should this occur, it could lead to delayed access to or even loss of reserves, inability to access assets, and/or liquidity shortfalls. **Legal Risk**: Changes in laws, enforcement priorities, or interpretations of the applicable legal frameworks may limit, delay, or restrict activities by the Issuer resulting in reduced fulfillment of the Issuer's Purpose as described in field A.13.
I.3	Crypto-Assets-related Risks	**Risk of limitation or loss of the Tokens' functionalities:** The Tokens do not grant their holder any rights vis-à-vis the Issuer, but merely offer the functionalities intended use in the ZKsync ecosystem ascribed to them from time to time (currently exclusively participation in the Governance Procedures). The Issuer cannot rule out, and ultimately cannot prevent, the possibility that the functionalities offered by the Tokens could be restricted in the future (e.g., via community votes through the Governance Procedures). The Issuer expects that any such limitation or loss of the functionality of the Tokens would lead to a negative change in the market valuation of the Tokens, which could result in a total or partial loss of a Token holder's investment. **Risk of Loss of (access to) the Tokens:** Token holders could lose their Tokens (or access to them) in a variety of ways. These include, for example, (i) loss/theft/damage to the hardware

No.	Field	Content Reported
		wallet in which the private key is stored, (ii) loss/theft of the private key or seed (recovery) phrase for the wallet, (iii) issues resulting from using a centralized custody provider (technical failure/insolvency/misuse), (iv) malfunction of a smart contract, (v) hacker attacks, etc. All of these can in themselves lead to a total or partial loss of a token holder's investment. **Risk of Financial Loss**: Trading crypto-assets can result in substantial losses. In the worst case, the Token holders could experience a total loss of their investment. **Risk of High Volatility**: Tokens do not convey any claims or rights beyond ownership rights and are not backed by physical assets. Their market value depends entirely on the expectation of future and sustained interest of persons buying the Tokens. The Token holders may face an illiquid, highly volatile, and unpredictable secondary market, leading to rapid increases or decreases in the value of the Tokens. The correlation between market expectations and the value of the Tokens can increase the likelihood of speculation-driven pricing, known as "momentum pricing". **Abrupt Market Events**: The value of the Tokens may be (temporarily or permanently) negatively affected by ad-hoc political or economic events domestically or internationally. **Liquidity Risk**: The Issuer cannot and will not guarantee that there will be an active and liquid secondary market allowing the Token holders to sell their Tokens to third parties, such as counterparties, brokers, liquidity providers, or other investors. Liquidity in the Tokens can be significantly lower than in other financial instruments, such as listed stocks or major currencies. This may hinder the Token holder from satisfactorily selling or buying Tokens or achieving satisfactory trading results, respectively. **Market Abuse Risks**: While MiCAR introduced a regime that is aimed at ensuring market integrity, secondary market transactions in the Tokens remain subject to behavioral risks, including fraud, deception, misleading information, lack of price transparency, and other malicious activities. **Regulatory Risk**: Changes to regulatory or supervisory frameworks applicable to the Tokens can lead to temporary or long-term interruptions in trading or settlement processes. Further regulatory risk stems from the fact that crypto-assets in general and thereto-related crypto-asset services are unregulated in certain jurisdictions outside of the EU/EEA, potentially leading to diverging regulatory treatment of the Tokens across non-EU/EEA countries. **ESG-related Risk**: Environmental, social, or governance (ESG) aspects related to the Token, particularly regarding the

No.	Field	Content Reported
		underlying technology and energy consumption, may conflict with the ESG preferences of Token holders. **Taxation Risk**: The transactions in the Token in general will be subject to taxation regimes that may significantly vary from one jurisdiction to another. In addition, the qualification of the Token under applicable tax rules may negatively affect the tax treatment of such transactions in the respective country.
I.4	Project Implementation-Related Risks	**Financial Risk**: Financial condition of ZKsync Protocol development organizations, which include the other legal persons involved in the implementation of the crypto-asset project defined in D.5 (the "**ZKsync Protocol Development Organizations**"): A material adverse change in the financial condition of supporting protocol development organizations could impact the ability to fund development and contribute to the ZKsync ecosystem, potentially eroding trust and affecting the ZKsync protocol's growth. This could potentially erode trust in the Issuer and affect the value of the Token. **Risk of Reliance on Key Personnel in ZKsync Protocol Development Organizations**: The ZKsync protocol's ongoing development and maintenance is substantially dependent on the expertise of the supporting protocol development organizations. The loss of key personnel in these supporting organizations could adversely impact the protocol's innovation and stability resulting e.g. in limited Token functionality and also affect the value of the Token. **Operational & Security Risks of ZKsync Protocol Development Organizations**: A failure of internal controls, a cybersecurity breach, or other operational failure at protocol development organizations could disrupt development or, in a worst-case scenario, compromise assets or systems under its direct control before they are fully decentralized. **Conflicts of Interest of ZKsync Protocol Development Organizations**: Matter Labs investors and team members hold a significant allocation of Tokens, and their financial interests may not always align with those of other Token holders. This could influence their participation in Governance Procedures or other actions. **Decreased Project Interest**: development of ZKsync relies on the interest and contributions by external actors, e.g. actors proposing and voting on protocol upgrades and also general acceptance of the ZKsync ecosystem. A decline of such activity might lead to a decline of further developments of the project and affect Token price. **Sanctions and AML Compliance Risk:** There is a risk that airdrop distributions or governance participation may inadvertently involve persons or entities subject to international sanctions or

No.	Field	Content Reported
		AML restrictions. This could expose the Issuer and associated protocol development organizations to regulatory liability, reputational harm, and potential enforcement action. Screening processes in place as technical mitigations, see also I.6, may yield false positives or negatives, leading either to the wrongful exclusion of eligible participants or the accidental inclusion of restricted persons. Such outcomes may impair the inclusiveness to protocol participation and hinder adoption of the protocol. **Regulatory Risk**: If the project faces new, unexpected (changes to) regulatory frameworks, this could delay project implementation or, in a worst-case-scenario, cancellation.
I.5	Technology-Related Risks	**Sequencer Risk & Liveness Attacks**: ZKsync currently operates with a single sequencer, which is responsible for ordering transactions and submitting them to the rollup contract on Ethereum. While this design enables high throughput and low latency, it introduces a potential single point of failure. If the sequencer becomes unavailable or malicious, transaction inclusion may be delayed. This could temporarily or permanently damage the reputation of the ZKsync ecosystem, lead to a decline in interest in the ZKsync ecosystem, and indirectly also lead to a negative development for the market valuation of the token. While the Governance Procedures allow for the selection of a new sequencer, it cannot be guaranteed that such a switch to a new sequencer could be successfully implemented. **Proof Generation & Verifier Bugs**: ZKsync relies on complex zero-knowledge cryptography to compress and prove large batches of transactions. Bugs in the circuit logic, proof construction, or verification code could pose risks to data integrity and state correctness. Implementation errors could compromise the rollup's correctness or halt proof submission to Ethereum. **Code Quality and Deployment Risks**: Like all software systems, ZKsync protocol is susceptible to bugs introduced in protocol upgrades or new smart contract deployments. Errors in upgrade logic, cross-version compatibility, or permission settings could lead to unintended consequences such as fund lockups, degraded functionality, or vulnerabilities exploitable by adversaries. **Data Availability Risks**: Although ZKsync posts transaction data to Ethereum (ensuring "on-chain" data availability), transitions to off-chain data availability schemes (e.g., Volition or Validium modes) would introduce new assumptions and risks. If data is withheld or becomes unavailable, users may be unable to reconstruct the rollup state or prove exits, depending on the chosen data availability model.

No.	Field	Content Reported
		Cryptographic Assumption Risks (incl. Quantum Threats): The integrity of ZKsync's system depends on cryptographic assumptions that currently underpin zero-knowledge proofs and Ethereum security. If future advances in quantum computing undermine elliptic curve cryptography or SNARK/STARK schemes, the security model would require proactive adaptation through cryptographic migration plans. **Interoperability & Ecosystem Dependencies**: ZKsync is integrated into the Ethereum ecosystem. Its success depends on composability with existing Ethereum tools (e.g., wallets, bridges, dApps) and compatibility with upgrades such as EIP-4844 (Proto-Danksharding). Any delays or forks in Ethereum's roadmap may affect ZKsync's performance, scalability, and long-term evolution. **Denial-of-Service (DOS) and Network Partition Attacks**: Although the underlying rollup design is resilient to many traditional consensus attacks, ZKsync infrastructure—especially API endpoints, RPC gateways, and bridges—remains exposed to denial-of-service attacks or network partitioning attempts. These could degrade the user experience or temporarily prevent interaction with the rollup. **Upgrade and Governance Risks**: ZKsync has introduced governance mechanisms to support protocol upgrades and sequencer decentralization. Errors in governance logic, upgrade design, or adversarial governance capture could introduce risk to the system's reliability and alignment with community expectations. **Blockchain Risks**: Blockchain networks are generally subject to constant development and change. Their open source nature and the use of smart contracts can make them susceptible to technical vulnerabilities that could lead to a general network disruption. For Token holders, such disruption can have a variety of negative consequences, including the delay or inability to proceed with a transaction or settle a transaction, inability to access funds, or a major loss. **Cyber Risk**: Distributed ledger technology and smart contracts may be subject to malicious cyber-attacks. These may include the exploitation of technical vulnerabilities in order to steal digitally stored passwords, private keys, and/or decryption keys to access certain data or assets. **Smart Contract Risks**: Smart contracts may encounter a coding error or a technical vulnerability, which can ultimately result in losses for Token holders. **Risks related to Ethereum:** There is no guarantee or assurance that the network of nodes on Ethereum performing the validation of transactions will allocate the crypto-assets according to the transfers initiated to or from the crypto-asset

No.	Field	Content Reported
		holder, as proposed in the respective conditions. One or more validators who gain control over a significant portion of nodes of the network can defraud other users by manipulating the database and making it the authoritative version of the database to initiate additional transfers based on the manipulations (51% attacks). **Risk of Irreversibility of Transactions**: Transactions involving digital assets on a blockchain are irreversible and final, and the transaction history cannot be altered by computer means. Therefore, an erroneous transaction (e.g., the transfer of Tokens using an incorrect digital ledger address) cannot be reversed, canceled, or corrected. **Forking risk:** The Tokens may be subject to a "fork" where the blockchain splits into two separate blockchains with a different consensus. Such forks can lead, among other things, to the creation of new or competing digital assets, impair functionality, convertibility, or transferability, or result in a complete or partial loss of holdings or a devaluation (including a reduction to zero) of the holder's Tokens. **Unanticipated Risks**: 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 within this section.
I.6	Mitigation measures	**Due Diligence**: Issuer and the ZKsync Protocol Development Organizations conduct thorough due diligence applying industry-standards when selecting third-party service providers for e.g. code audits or penetration testing. **Audits**: independent smart contract and protocol audits are performed by reputable (third-party) security firms prior to deployment of any major upgrade. Regular penetration testing, code reviews and bug bounty programs are conducted to identify and address vulnerabilities in smart contracts, cryptographic primitives, and infrastructure. Continuous monitoring of deployed contracts enables early detection of anomalies or suspicious activity. These measures reduce the likelihood of technical failures, exploitation, or systemic risks to the protocol and its users. **Governance system featuring veto rights, Security Council, Guardians**: The governance system outlined in the Governance Procedures incorporates layers to mitigate risks arising from malicious governance actions or protocol-level failures. • **Security Council**: The Security Council serves as an independent body with the mandate to safeguard the security of the ZKsync protocol. It holds emergency powers to (i) freeze the protocol in response to imminent or active security threats, such as critical bugs or

No.	Field	Content Reported
		exploits, that could jeopardize the integrity of the protocol, (ii) initiate emergency protocol upgrades and (iii) refuse to execute governance proposals as outlined in the ZKsync Governance Procedures due to security requirements. • **Guardians**: The Guardians have the independent authority to veto governance proposals that conflict with the values and principles of the ZK Credo, available at https://github.com/zksync/credo (last accessed: 2025-09-24). This includes the right to block proposals deemed abusive, malicious, or otherwise detrimental to ZKsync or its governance system. **Decentralized contributions to ZKsync development**: Risk mitigation is further reinforced by the distributed nature of contributions to ZKsync development. Independent teams and contributors actively participate in protocol design, research, review, and implementation. This decentralization reduces concentration risk, avoids reliance on a single development entity, and fosters peer review across a broad set of stakeholders. **Emergency Response Procedures**: ZKsync maintains predefined emergency protocols, as defined in the ZKsync Governance Procedures, to address critical incidents such as contract exploits, consensus failures, or systemic anomalies. Incident detection is supported by continuous on-chain monitoring and alerting systems, enabling rapid escalation to relevant governance bodies. Coordinated response playbooks, including disclosure guidelines and patch deployment processes, ensure timely response. **Additional Security Reviews and Bug Bounty Programs**: To ensure mathematical soundness and robustness, ZK-proofs used within ZKsync are subject to continuous security reviews, bug bounty programs, and rigorous testing frameworks. These processes substantially mitigate risks of fraud proofs being invalid, ensure transaction integrity, and enhance overall trust in the security of the protocol.

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

[Information referred to in the Annex to Commission Delegated Regulation (EU) 2025/422 specifying the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the climate and other environment-related adverse impacts].

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

No.	Field	Content Reported
General Information		
S.1	Name	ZKsync Association
S.2	Relevant legal entity identifier	529900SV858GPLFCQK64
S.3	Name of the crypto- asset	ZKsync (ZK)
S.4	Consensus Mechanism	See item H.5.
S.5	Incentive Mechanisms and Applicable Fees	See item H.5.
S.6	Beginning of the period to which the disclosure relates	2024-08-28
S.7	End of the period to which the disclosure relates	2025-08-27
Mandatory key indicator on energy consumption		
S.8	Energy consumption	156,476.7 kWh
Sources and methodologies		
S.9	Energy consumption	The data and analysis methodology for energy consumption was sourced from CCRI (last accessed: 2025-09-24).

No.	Field	Content Reported
	sources and methodologies	

2. Supplementary information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

No.	Field	Content Reported
S.10 – S.16	[intentionally left blank]	The energy consumption reported in field S.8. is less than 500,000 kWh per calendar year. Thus, the information in fields S.10 to S.16 can (and will) be omitted in accordance with Art 4 para 2 of Commission Delegated Regulation (EU) 2025/422.

3. Optional information on principal adverse impacts on the climate and on other environment-related adverse impacts of the consensus mechanism

No.	Field	Content Reported
S.17 – S.36	[intentionally left blank]	In accordance with Art 4 para 3 of Commission Delegated Regulation (EU) 2025/422, the (voluntary) inclusion of information in fields S.17 to S.36 is omitted.