




**CRYPTOMERIA  
CAPITAL**

In corporate partnership with AXON 

# STATE OF ZERO KNOWLEDGE 2023

**November 2023**

# DEAR PARTNERS, INVESTORS, AND FRIENDS

“

We are honoured to present this new extensive analysis of the Zero-Knowledge technologies landscape, where we have collected observations of major changes and developments in the field up to the current date. As the demand for Ethereum scaling solutions continues to rise, an increasing number of projects aimed at enhancing security, privacy, and speed of the protocols are emerging in the market.

Complemented by the unique insights and findings, the report provides an overview of the current state of Layer 1 and Layer 2 scalability solutions and ecosystems, becoming an indispensable guide to the upcoming bull market for everyone interested in Zero-Knowledge technologies. Within this report, we have placed special emphasis on ZK-rollups—a technology enabling private and secure off-chain transaction aggregation, reducing transaction fees, and improving transaction throughput. ZK-rollup technology holds immense potential to transform the entire cryptocurrency ecosystem, playing a major role in the future of Web3, decentralized finance, and the metaverse. With the hope that this analysis will equip you with essential information, we wish you an enlightening and insightful reading.

”



**VADIM KREKOTIN**

Founding Partner at  
Cryptomeria Capital

## RESEARCH PARTNERS

Linea<sup>o</sup>

 Scroll

 zkSync

 taiko

 MANTA  
NETWORK

 oLabs

 ALILAYER

 STARKNET

 KROMA

 Kakarot

 CYSIC

 IOSG  
VENTURES

 INTMAX

 SPACE SHARD

INTELLECTUAL PARTNER

ARTHUR  LITTLE

## MEDIA PARTNERS

 METVERSE  
POST

 @mpost\_io

**ZK SEASONS**  
Community Events Worldwide

 @zkseasons

 STARKNETICS  
All Starknet Ecosystem in your pocket

 @Starknetics

**Disclaimer:** Cryptomeria Capital does not impose any fees on its research partners. All integrations are complimentary, and the report is intended solely as a public good.

# CONTENTS

<b>1. Key takeaways</b>	<b>5</b>
<b>2. Current ZK Rollups Landscape</b>	<b>6</b>
I. zkSync	6
II. StarkNet	16
III. Scroll	23
<b>a. Arthur D. Little</b>	<b>30</b>
IV. Aztec Network	32
V. Polygon	36
VI. Taiko	44
VII. Linea	50
VIII. Loopring	57
IX. Kroma	62
X. Manta Network	69
<b>b. ZK Seasons - Taking ZK Networking to the Next Level</b>	<b>76</b>
<b>3. Current ZK Layer 1 Landscape</b>	<b>77</b>
I. Mina	77
<b>c. IOSG Ventures</b>	<b>82</b>
II. Aleo	84
<b>4. Core Discussions on ZK</b>	<b>88</b>
I. Market Adoption	88
II. ZKP Hardware	94
III. ZKML	99
IV. Decentralisation of the Sequencer	103
<b>d. AltLayer</b>	<b>106</b>
<b>5. Conclusions</b>	<b>108</b>
<b>6. About the Authors</b>	<b>110</b>
<b>7. Bibliography</b>	<b>111</b>



# KEY TAKEAWAYS

- Within the field of Zero-Knowledge solutions, the sectors of Scaling and Privacy are of paramount importance. Privacy - particularly within domains like finance, personal data, deanonymization, location, health, and credit scores - remains a top concern for both individuals and organizations.
- EIP-4844, also known as Proto-Danksharding, is an upcoming milestone in the Ethereum "Cancun" upgrade. It aims to lower data availability costs for Rollups - enhancing data storage, ZK-proof generation, as well as circuit efficiency.
- Over the last 7 years, Web3 experienced significant growth in developer activity. By 2022, the number had reached over 61,000, marking a 66% increase compared to three years prior. Despite a notable 27% drop in developer numbers since October 2022, which can be largely attributed to newcomers, the overall trend remains positive. As of October 1, 2023, there are 19,300 monthly active open source developers.
- ASICs are set to provide powerful ZKP acceleration, while FPGAs cater to computationally intensive ZK use cases. Progress in ZKP schemes, coupled with hardware advancements, promises to enhance scalability, fees, privacy, and interoperability within Web3.
- In 2023, the ZK rollup ecosystem made strides in zkEVM functionality and EVM compatibility. The adoption of certain solutions by various projects indicates the rise of the first practical, universally applicable solutions in the sector. Simultaneously, we are witnessing the evolution of zkVMs, which serve as L2-focused development environments, providing a unique development experience.
- While still in its early stages of development, ZKML is anticipated to have applications in data security and secure ML model training. This includes Privacy-Preserved Model Evaluation, Computational Integrity, On-Chain Model Verification, as well as AI Oracle Proof creation.
- Efforts to tackle Sequencer challenges in blockchain systems are exploring various approaches, such as shared, outsourced, or dedicated Sequencer solutions, along with other progressive strategies. However, the effective implementation of these ideas is still in the developmental phase. Concepts like decentralized Sequencers Proof of Authority, Proof of Stake, Miner Extractable Value auctions, and Proof of Elapsed Time are currently in their early stages.



# 2 CURRENT ZK ROLLUPS LANDSCAPE

## I. ZKSYNC



### Introduction

zkSync is developed by Matter Labs ZKR and stands out with its native account abstraction and extensive EVM compatibility. This achievement is made possible through the implementation of a custom-designed zkVM, which offers convenient features for composing ZK code and enhances code compatibility.

The ecosystem comprises two key components: zkSync Era (ZK-rollup) and zkPorter (off-chain rollup). Also, they are actively working on infrastructure innovations like a modular network of Hyperchains, ZK Stack – out of the box solution for ZK-rollup setting and launching, and zk-STARK integration by Boojum ZKP upgrade.

zkSync facilitates 3,000 TPS and rapid cross-layer token transfers, guaranteeing instant confirmation and processing within 10 minutes. In contrast, zkPorter Validium unlocks even higher scalability potential boasting up to 20,000+ TPS.

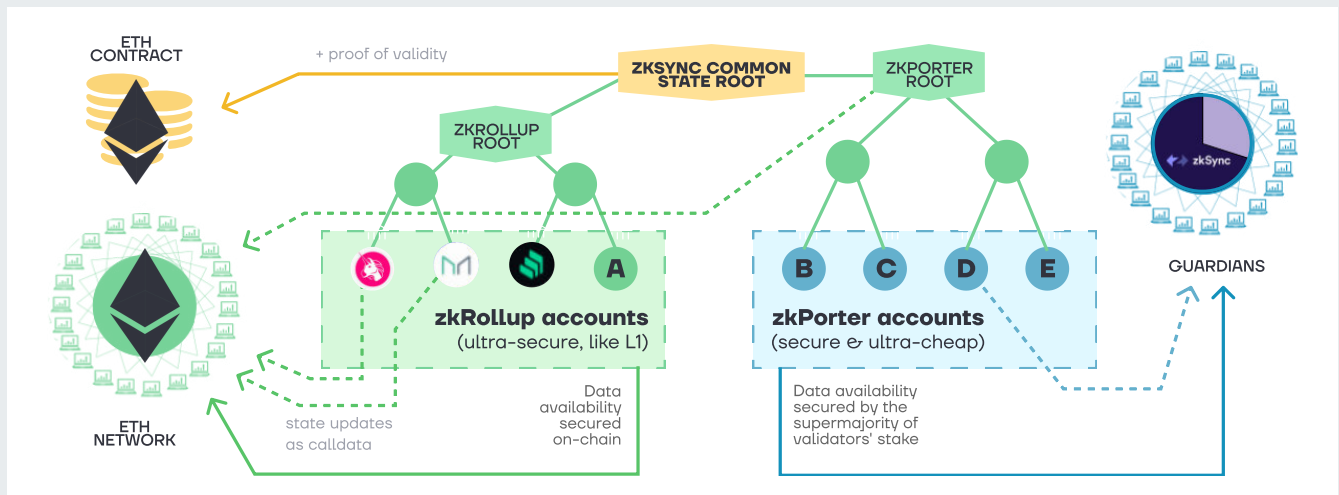


Figure 1. zkPorter and zkSync Rollups scheme.

Source: Matter Labs: "zkPorter: A Breakthrough in L2 Scaling".

### Architecture and Fundamental Components

#### • Account Abstraction (AA) and Paymasters

zkSync Era has native AA from day one, allowing users to work with smart contract accounts (CAs). Also, any account can be managed in L2 with the same private key that is used for L1. This eliminates reliance on third-party intermediaries and mitigates risks associated with Externally owned accounts (EOA), like storing of private keys and seeds.

AA is a fundamental block of the zkSync ecosystem, particularly when users and developers work with Hyperchains and Hyperbridges. It simplifies the complex underlying processes, making them user-friendly and accessible through an intuitive interface for deployment.

Built-in solution Paymasters empower any Era account to automate payments, cover fees in multiple tokens, and work fee-free with their dApps. Paymasters can facilitate ERC20 token-to-ETH conversions, enhancing UX. But it's important to note that Paymasters will not be a default option after the Mainnet launch to prevent an overflow of demand to privileged projects.

- **zkPorter**

Initially, zkPorter draws inspiration from Starkware's Volition and StarkEx architecture, which is hybrid on-chain/off-chain data solutions. zkSync Era and zkPorter seamlessly interact with each other, but they differ in terms of data storage and data availability concept. The first one ensures on-chain DA with data (state diffs) publishing to the Ethereum L1.

This is a potentially convenient solution for DeFi and DEX operations, and for Oracles. Also, zkPorter brings additional UX advantage of constant transaction costs that can be a setting option for dApps and smart contract creators. zkSync Era publishes only state differences instead of transaction inputs, which helps to achieve data compression and integration with zkPorter.

zkPorter employs DA and data storage off-chain with its own shards, block producers and safeguarded PoS. Users must choose with each zkPorter account whether to produce transactions with off-chain data availability.

Guardians (PoS stakers) work as a trustless Data Availability Committee (DAC) model, which means that they can be slashed for malicious behavior. Guardians stake zkSync tokens and sign blocks to confirm data availability in zkPorter accounts. That's type of DAC is good for security and decentralization, but have an open research problem issue that called Fisherman's Problem:

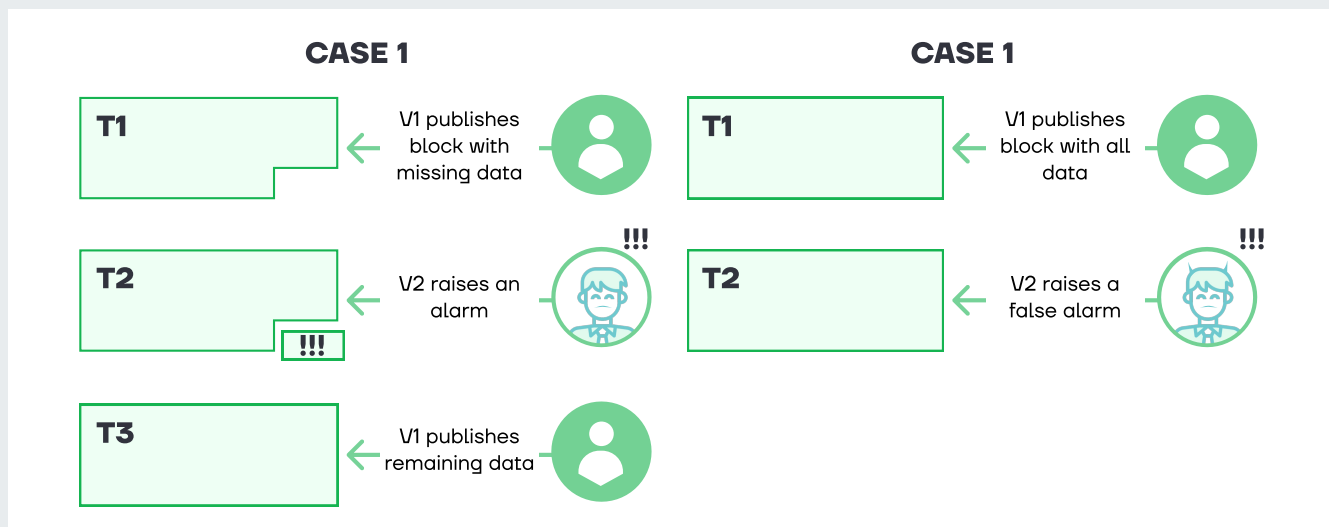


Figure 2. Data unavailability is not a uniquely attributable fault.

Source: Infura: "Solving Blockchain Scalability with DAC".

- **ZK Stack and Hyperchains**

The ZK Stack is a modular, free, open-source framework for building custom ZK-powered L2s and L3s. ZK Stack allows flexible design for Hyperchains, includes modules like: Sequencer, Circuits, Prover, System contracts, Bridging interfaces, Compiler, SDKs.

zkSync offers various deployment options, especially with DA layer settings for Hyperchains based on L2. Main requirements to launch a Hyperchain is implementation of the zkSync zkEVM and an in-built L2/L3 Sequencer, which can be driven by native PoS staking.

Cross-layer messaging enables the transmission of messages of arbitrary length between zkSync Era, Ethereum, and Hyperchains. This seamless cross-layer communication feature opens up a wide range of possibilities for developers, even when using separate rollups.

This setup enhances interoperability, scalability, and efficient asset transfers across multiple blockchain layers within the ecosystem and reshapes zkSync from a ZK rollup to a comprehensive modular infrastructure solution.

Hyperchains are interconnected through specialized Hyperbridges, enabling cross-layer transactions. These bridges leverage smart contracts to validate Merkle proofs of transactions, import transaction roots, and verify proofs on Layer 1 (L1). Each Hyperchain within the ecosystem operates independently, giving them sovereignty, and allowing optional proof aggregation. Hyperchains can settle their proofs directly to Ethereum, albeit at a higher fee.

Hyperchains have the flexibility to comprise one or more logical partitions residing within the same state but existing in separate subtrees. These partitions enforce distinct data availability policies while still having the capability to interoperate synchronously. Hyperchains can operate in different modes, such as Validium mode, similar to Layer 3 privacy protocols, or function as Self-hosted Rollups with Shared Bridge.

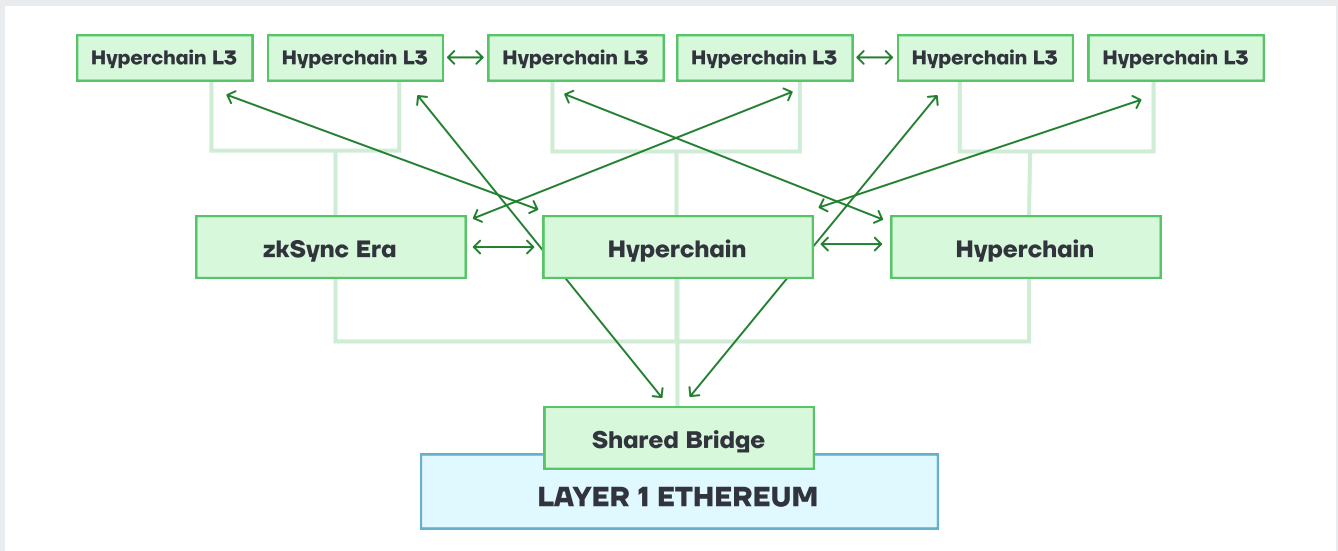


Figure 3. Hyperchains.  
Source: Era zkSync Documentation.

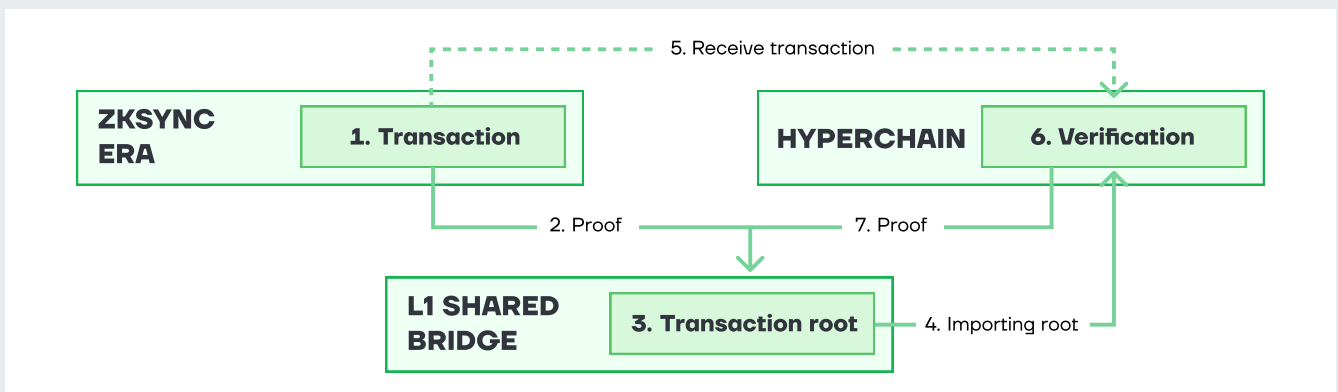


Figure 4. 7 steps of the Hyperbridging.  
Source: Era zkSync Documentation.



There are three types of bridge connections in zkSync's architecture: L2→L1 bridges (asynchronous and not atomic, functioning like a messaging), ZkPorter bridges (based on shards, atomic and asynchronous, designed mainly for developers), and Hyperbridges (L2→L2 and L2→L3, asynchronous and not atomic).

Hyperchains creators have the flexibility to choose the following architectures:

	Aggregation	L3S	Layered Aggregation
Fast Messaging	NO	YES	YES
Scales	YES	NO	YES
Consensus Mechanism	NO	L2 Full Consensus	Lightweight Consensus
Instant Messaging Add-on	NO	YES	YES
Sovereign	YES	YES	YES

Figure 5. Feature comparison of the different aggregator mechanisms.

Source: Era zkSync Documentation.

**1. Simple Aggregation:** This involves using a shared L2→L1 bridge to aggregate proofs from Hyperchains and send them directly to the Prover's smart contract on Ethereum Mainnet. This aggregation mechanism may not facilitate rapid messaging since proofs are seldom processed at the L1 level to save on gas fees.

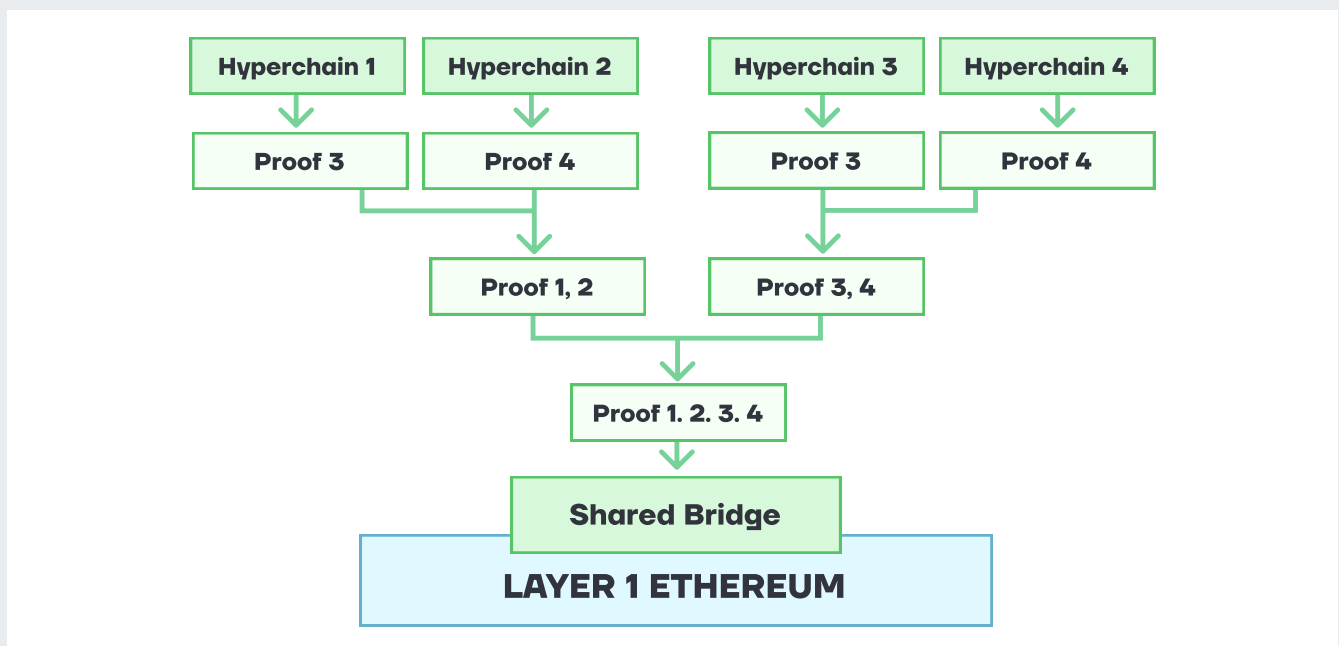


Figure 6. Simple proof aggregation.

Source: Era zkSync Documentation.

**2. L3 Aggregation:** This approach is well-suited for Validiums that don't need to offload data to L1. It allows for the creation of a shared DA layer based on the chosen L2, provided there is a dedicated Prover on L3. While this approach has load limits for proof verification on L2, it offers high-speed interactions between adjacent L3 layers and cost-effective transactions. Proofs are generated in parallel on L1 and transmitted without delay for off-chain transaction verification.

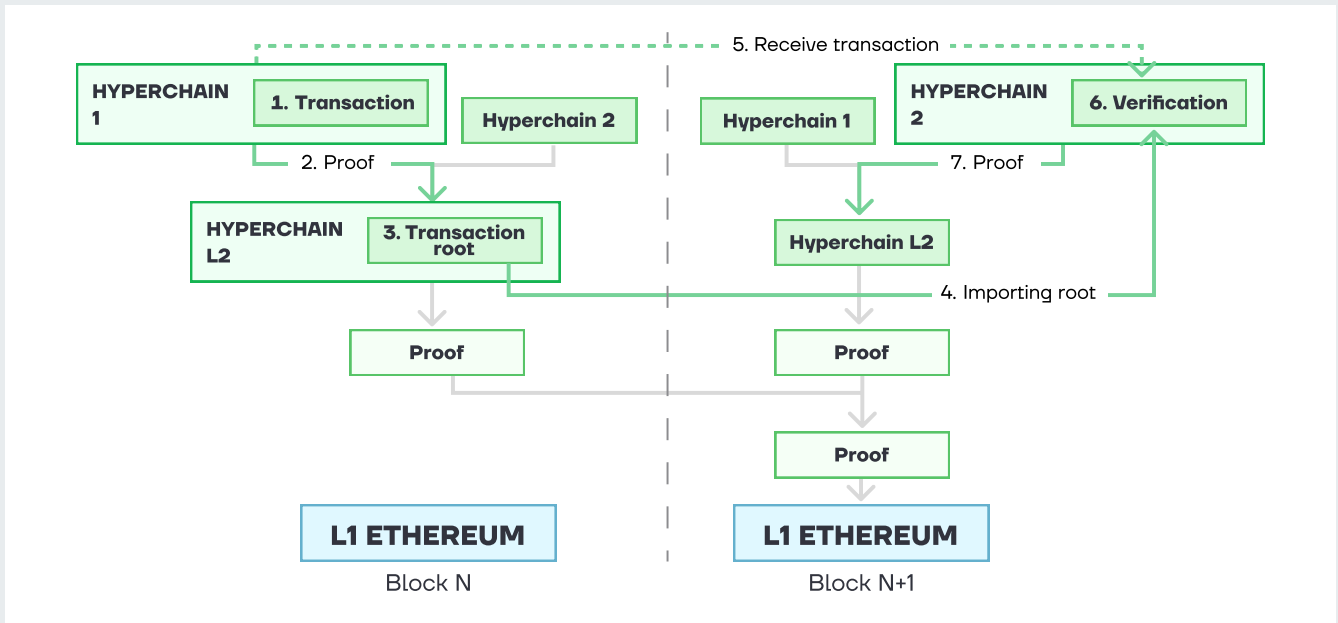


Figure 7. L3s.  
Source: Era zkSync Documentation.

**3. Layered Aggregation:** This simplifies the L3 aggregation system by introducing L3 messaging as an alternative to L2 proof computation. By monitoring the State Root of participants' rollups, the Transaction Root is identified and packed into a "special" proof. Through aggregation, it is sent along with other proofs to L1.

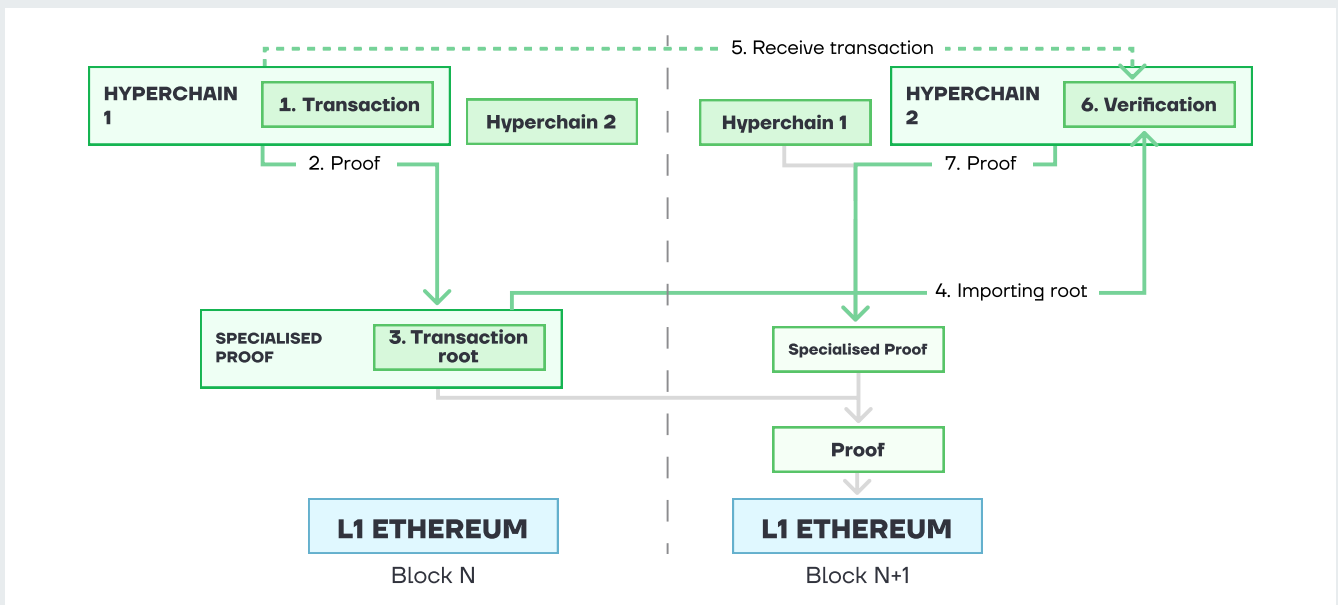


Figure 8. Layered Aggregation.  
Source: Era zkSync Documentation.

## • From SNARKS to STARKS

zkSync's default zk-SNARKs rely on the altbn128 elliptic curve, currently secure but don't have quantum resistance. They employ the PLONK proving scheme with KZG commitments, which offers good computational speed and cost-efficiency and can be updated without problems.

Security system means that submitting an invalid block to the rollup requires bypassing both the cryptography and the Sequencer/PoS consensus mechanisms. So, to enhance security on the ZKP side, zkSync employs a two-pronged architecture approach:

1. Isolation: Only blocks authorized by a designated Sequencer can commit state transitions to the zkSync Layer 1 smart contract. There are plans to transition to a collective Sequencer protected by a multi-validator consensus using Proof of Stake. Now, the system's security code and Verifier contract can be modified only after approval from 4/8 Multisig participants.
2. Redundancy: Every transaction sent to the Sequencer(s) undergoes validation through simple execution before inclusion in a block. This redundancy layer adds extra protection against vulnerabilities and exploits within the zkSync ecosystem.

After a long time, zkSync announced their Redfish cryptographic upgrade called Boojum. It's a STARK-based proof system that employs PLONK arithmetization with FRI as the commitment scheme (Firstly implemented in Starkware zk-STARK). Some components for the new proof system were implemented from the Polygon Zero Plonky2 solution, and now everyone can see the open-source code of the Boojum to use or improve it.

One of the challenges in implementing post-quantum SNARKs like Boojum is the need to balance security with verification costs, which tend to increase linearly with enhanced security. zkSync addresses this by optimizing proof size and leveraging the FRI protocol, achieving a reasonable equilibrium between Verifier cost and Prover speed, ensuring both security and scalability.

While the new proof scheme and codebase are still in development and undergoing off-chain testing, they are already capable of generating and verifying L2 blocks. This parallel testing with the existing zk-SNARKS scheme is a crucial step in zkSync's evolution.

Transitioning to a new system like Boojum presents challenges for users, but zkSync is actively working on solutions to facilitate a smooth transition and maintain system stability. In the final phase of the Boojum update, zkSync plans to encapsulate STARK proofs within a non-transparent pairing-based SNARK, reducing verification costs and overall transaction expenses on the Ethereum L1, enhancing efficiency and cost-effectiveness for users.

Currently, Boojum is testing in "Shadow proving" mode on the zkSync Era Mainnet. This solution is vital in implementing ZK Circuits and the ZK Stack.

To find more about zkSync architecture, refer to the [ZK Rollups Landscape report](#) (page 24).

## EVM-Compatibility and Privacy

- **zkSync zkEVM**

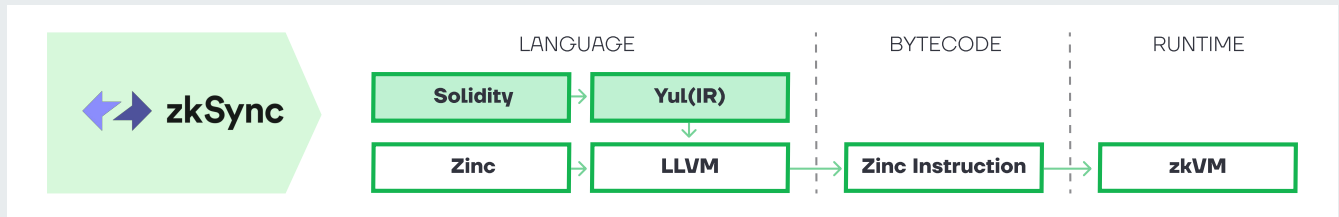


Figure 9. zkSync zkEVM.

Source: zkValidator: “zkEVMs Beyond Polygon and zkSync”.

It is a Type 4 zkEVM based on Vitalik Buterin's framework, which offers fast Prover times and easy adoption for developers. However, it has some issues, like incompatibility with handwritten EVM bytecode, which may limit compatibility with dApps and Web3 tools. Despite these issues, zkSync demonstrates ecosystem growth and remains developer-friendly.

zkSync prioritizes speed in proof generation over aiming for EVM equivalence. They achieve this through a custom LLVM compiler that supports Solidity, Vyper, and Yul. LLVM is a special solution that provides a zk circuit compiler. Thanks to LLVM, we can see the adoption of Rust and other high-level languages in the near the future.

zkEVM supports Ethereum cryptographic primitives, simplifies testing with a Hardhat plugin that has language-level equivalent, and improves UX with native account abstraction which can operate with Hyperchains.

Zinc – is the native zkSync language that is designed for building smart contracts and performing various computations, including ZKP generation. It has Rust syntax and the code is designed immutability that ensures safe math to create cleaner smart contracts.

Zinc, despite its limitations such as the absence of unbounded loops or recursion, offers significant advantages. It simplifies code debugging, offers versatile project management, build, test, and benchmarking options, and maintains compatibility with Solidity. Additionally, an experimental transpiler known as Soul Z facilitates the automated conversion of Solidity contracts into Zinc with minimal required modifications.

- **CAPE for private transactions**

The zkSync team initially focused on achieving high scalability at minimal cost before native privacy features that are expensive for Provers at default. However, in January 2023, they announced a new private technology CAPE in collaboration with Espresso Systems to enable private transactions on zkSync.

This collaboration introduced CAPE, a smart contract application that allows users to customize access to custody and transfer data for their assets while ensuring transactions don't disclose private information on the public blockchain. Users can create new tokens or wrap existing ERC-20 tokens, tailoring them to specific privacy requirements. Asset creators gain the flexibility to set viewing policies for their assets, including sender and receiver addresses, asset quantities, and asset types. CAPE delivers precise control over asset privacy and transparency, elevating security and customization within the zkSync ecosystem.

# Ecosystem

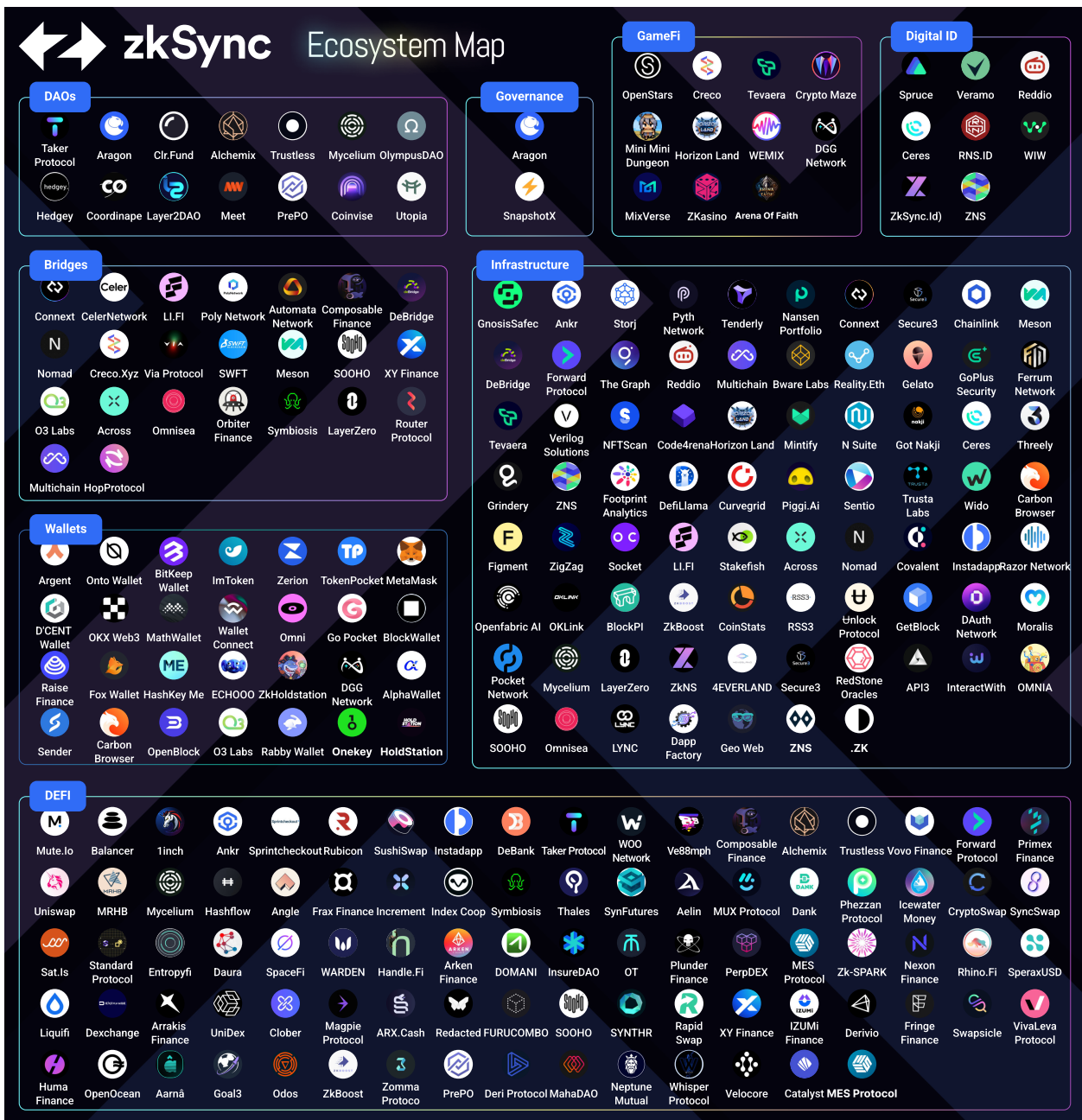


Figure 10. zkSync Ecosystem.  
Source: Cryptomeria Capital.

## Roadmap

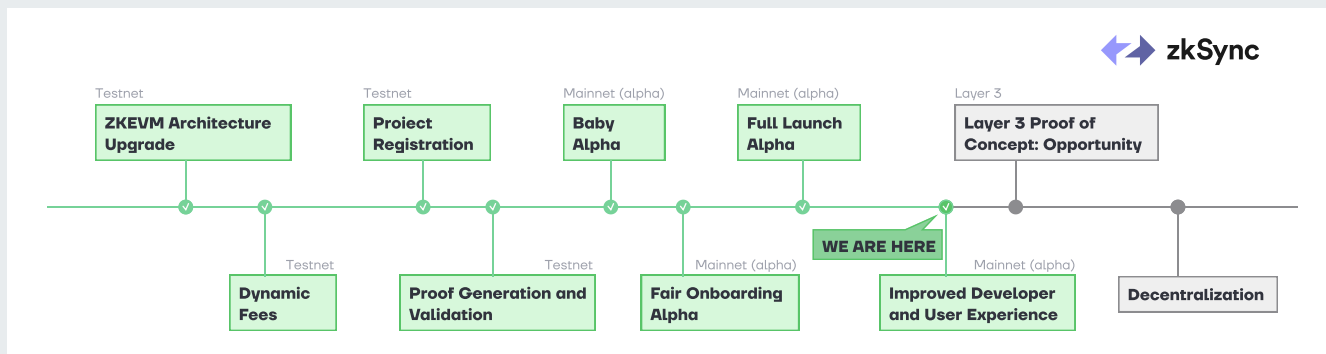


Figure 11. zkSync Roadmap.

Source: zkSync Documentation.

- **February 2022** - zkSync Lite launch on a public testnet — the first ever zkEVM implementation.
- **May 2022** - first zkEVM architecture upgrade. Major architecture overhaul, implementation of account abstraction and future feature support. It was a large-scale network upgrade.
- **July 2022** - upgrade for older versions of tools so developers didn't need to upgrade to use zkSync 2.0. Especially Vyper and Solidity support made it easier.
- **Summer 2022** - upgrade of fee modeling system.
- **Early Fall 2022** - merge of the Prover.
- **March 2023** - zkSync Era is in Full Alpha Mainnet, offering zkEVM, zkPorter, and Account Abstraction to all users and developers. It supports smart contracts based on Zinc and zkEVM with Solidity, Vyper, and Yul compilation.

### Next notable developments include:

- zkSync 3.0 update
- Decentralised Sequencer
- 2FA is switched to PoS-secured consensus
- Trustless mechanism implementation

## Conclusion

zkSync, developed by Matter Labs ZKR, is a prominent platform in the blockchain ecosystem, primarily due to its zkVM and extensive EVM compatibility. The platform encompasses two primary components: zkSync Era, a ZK-rollup solution, and zkPorter, an off-chain rollup.

While zkSync facilitates a throughput of 3,000 TPS with quick cross-layer token transfers, zkPorter promises an even higher scalability potential with over 20,000 TPS. zkSync's Account Abstraction feature allows users to interact effortlessly with smart contract accounts, using the same private keys for both Layer 1 and Layer 2. Another unique feature is Paymasters, which streamlines automated payments and fee coverage for users. The ecosystem also integrates with the modular network of Hyperchains and offers ZK Stack, an out-of-the-box solution for ZK-rollup configurations, enhancing the platform's flexibility and scalability.

One of zkSync's defining attributes is its dedication to infrastructure advancements. The introduction of Hyperchains and Hyperbridges has transformed zkSync from a mere ZK-rollup to an extensive modular infrastructure solution, boosting interoperability and efficient asset transfers across multiple blockchain layers. The platform's architecture includes diverse bridge connections, allowing seamless communication across layers. zkSync's zkEVM, inspired by Vitalik Buterin's framework, prioritizes proof generation speed and features an LLVM compiler, supporting multiple languages and promoting easy developer adoption. Additionally, zkSync has introduced its native language, Zinc, tailored for creating smart contracts and performing ZK proof generation. This language ensures safer and more efficient smart contract creation, even with certain limitations.

While zkSync initially emphasized scalability and cost-effectiveness, the introduction of the CAPE technology in partnership with Espresso Systems has pivoted its focus towards transactional privacy. CAPE enables private transactions, allowing users to customize data access for their assets, thereby ensuring non-disclosure of private transactional information on the public blockchain. Users have the flexibility to create new tokens or wrap existing ones, customizing them based on specific privacy needs. This move underlines zkSync's commitment to maintaining a balance between scalability, efficiency, and privacy. With its continuous innovations, zkSync is poised to redefine the blockchain landscape, promising a harmonious blend of speed, security, and user-centric features.

“

In 2023, the blockchain industry experienced a significant surge in interest and activity related to the Zero-Knowledge proof method and ZK-rollup scaling solutions. Despite facing market challenges, ZK-rollup technologies gained substantial momentum, leading to a shift in user engagement from Optimistic rollups. Several new Layer 2 networks, such as zkSync Era, Linea, Base, Starknet, and Scroll, were introduced, highlighting ZK-rollup solutions' rapid technological advancements and widespread user adoption.

While the Ethereum ecosystem has been displaying continued growth, this year marked a collective endeavour to reshape the landscape and reinforce Layer 2 infrastructure, thereby earning the designation of the "Year of Layer 2" in the realm of cryptocurrency and Web3.

”



**IVAN SEMENOV**

Managing Partner at Cryptomeria Capital

### Introduction

Starknet, a Validity Rollup, employs the Cairo VM, which comprises OpCodes tailored for the STARK proof system. This design specifically enhances the efficiency of Validity proofs. In Starknet, transaction statuses such as "submitted" and "accepted on L2" ensure off-chain security, while the status "accepted on L1" assures Ethereum security.

Starknet natively supports account abstraction to streamline the process of sending transactions. This includes security measures and social recovery, among other things. These features greatly improve the user experience when interacting with wallets. It is important to note that the Starknet deployment is currently permissionless.

In the present version, where the Sequencer is centrally managed by StarkWare, the cost of deposited transactions is determined solely by their execution cost.

Starknet's current state can be entirely derived from Ethereum. State differences between transitions are conveyed on L1 as call data (state diffs) and are published in a sequential order. Reconstructing the state is achieved by reading them sequentially, and this process is facilitated by Pathfinder, a full node client of Starknet.

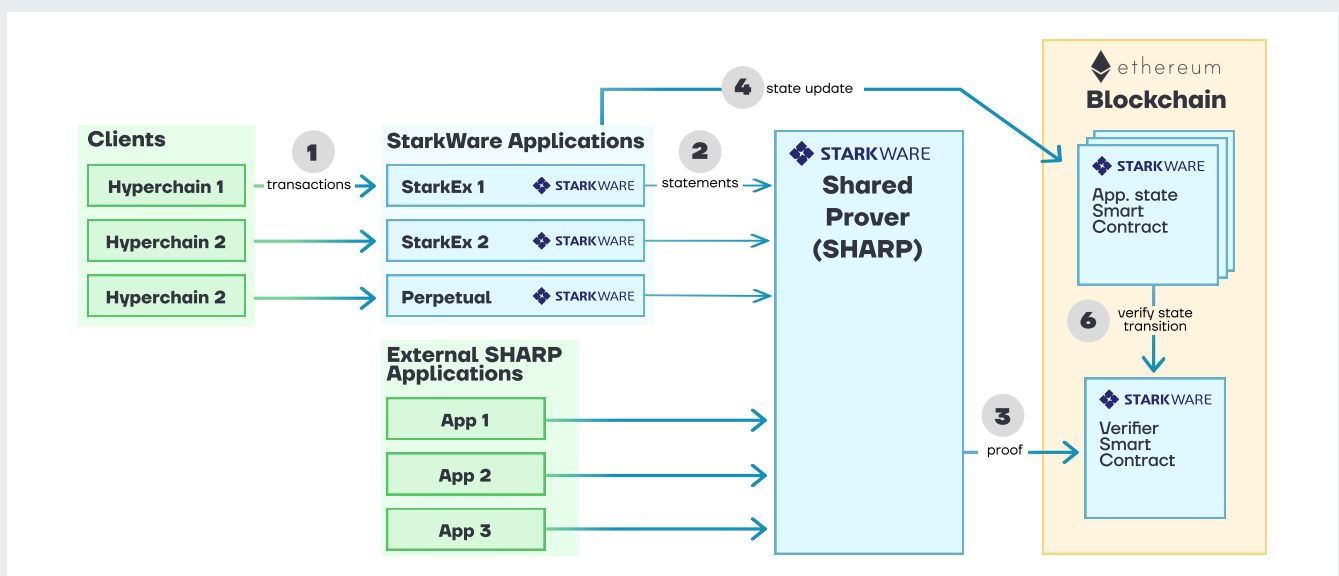


Figure 12. StarkWare services High-level architecture.

Source: StarkEx Documentation.

### Architecture and Fundamental Components

- **Account Abstraction (AA)**

Starknet embraces AA as its core principle, where all accounts are smart accounts, eliminating the existence of EOAs. This marks a shift towards a world where every account possesses smart capabilities, someone even with in-built Multisig frameworks.



The entire infrastructure, including wallets and block explorers, is meticulously designed and tailored for AA. Starknet noticed three key AA components: Signature Abstraction (freedom to customize account permissions), Fee Abstraction (different tokens can be used as payment for transaction fees), Nonce Abstraction (seamless, efficient, and user-friendly experience).

Notably, Visa has embarked on exploring "auto payments for self-custodial wallets" and a new type of account contract based on Starknet known as a "delegable account". The concept involves extending programmable validity rules for transactions, including a pre-approved allow list. Essentially, AA allows Visa to delegate the authority to instruct a user's account for initiating push payments to a pre-approved smart contract designed for auto payments.

- **StarkEx, Volition and DAC**

	Validity Proofs		Fault Proofs
Data On-Chain	Volition	ZK-Rollup	Optimistic Rollup
Data Off-Chain		Validium	Plasma

Figure 13. Volition options.

Source: Starkware: "Volition and the Emerging Data Availability".

StarkEx is a self-custodial scalability engine that is currently being actively implemented. The initial version of StarkEx enabled the deployment of an additional infrastructure layer for dApps. This layer could be implemented as a separate Rollup (with on-chain data) or as a Validium (with off-chain data), and as Volition (with hybrid data).

Starting from H2 2022, StarkEx 4.5 introduces support for Transaction Bundling and adds the Volition protocol for practical usage. Networks based on StarkEx can store transaction data off-chain, providing L1/L2 security guarantees and enabling better scaling opportunities. Volition allows users to combine on-chain and off-chain data storage, providing flexibility in choosing how to store data for each transaction. Transactions are batched and sent to SHARP for zk-STARK proof generation. Once generated, Verifier approves the validity of the state transitions on-chain.

Instead of zkSync's zkPorter scheme, StarkEx solution allows a user to choose the option of off-chain data availability for each transaction within an account.

To configure DA (Data Availability) and data storage options, dApp creators can use a permissioned Data Availability Committee (DAC). This committee consists of a limited set of nodes that are responsible for storing copies of off-chain data and providing access when requested.

DAC members are also responsible for keeping off-chain data copies as backups for security reasons. This ensures the possibility of one-way withdrawals by the Application Smart Contract (ASC) in critical situations (Operators bug or exploiting).

The primary concern with permissioned DACs is the risk of third-party trust with limited nodes. However, Starkware aims to enhance privacy by encrypting the data stored by the DAC.

Currently, StarkEx has implemented various trading functions such as Spot and Perpetual, as well as DeFi functions. These functions can be white-labeled and connected to external APIs.

In October 2023, StarkEx had already achieved \$525M in TVL and \$1T in Cumulative Trading.

- **Layer 3-4 Scaling**

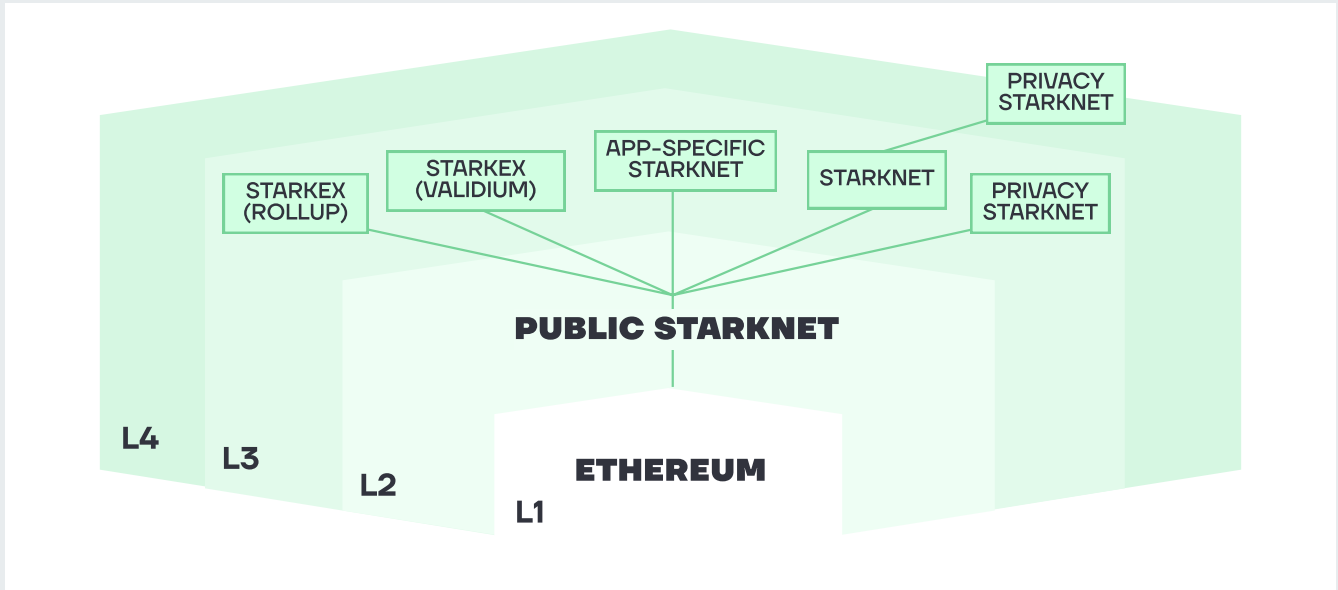


Figure 14. L3s and Fractal Layering.

Source: Starkware: “Fractal Scaling: From L2 to L3”.

The structure of additional layers on top of the main ZKR, presented in 2021, involves scaling by using a shared DA level. With this approach and efficient L1 <-> L2 messaging, Starknet can provide interconnectivity and scaling for Rollups and various StarkEx implementations. Also, L2/L3 chains can work as “Canary” networks for dApps or new ecosystems.

An additional feature is Madara, a built-in Sequencer optimized for Layer 3 and App chains. It is designed to execute transactions and group them into batches. Projects can choose to use Madara as an out-of-the-box solution or create their own Sequencer scheme.

- **Shared Prover (SHARP) and Verifier**

SHARP and the Verifier smart contract, developed by StarkWare, provide infrastructure for scalable applications by generating zk-STARK proofs for computational integrity statements. These proofs are stored on-chain in the Fact Registry, when customer applications commit their state on dedicated Ethereum-based smart contracts.

- **ZK-STARKS by StarkWare**

Starkware, founded by Ben-Sasson, Horesh, Riabzev, and Bentov, developed zk-STARK, a transparent proof system. This innovation allows blockchains to offload complex computations to a single STARK Prover. The verification of a STARK proof requires only a fraction of the computation, enabling the processing of multiple transactions off-chain. This approach reduces the computational burden on the Mainnet, resulting in lower transaction fees.

This ZKP approach is theoretically post-quantum and integrates zk-STARKs with a polynomial commitment scheme known as FRI, which was recently implemented in Boojum. This combination utilizes a technique called “grinding,” enhancing the cryptographic scheme’s robustness. However, it comes with increased maintenance costs for the Prover, which could potentially impact transaction fees price.

It is important to note that using FRI enables future improvements in the security features of the cryptographic component, but the operation cost of the SHARP Verifier will increase linearly. Therefore, Starknet can adjust its actions based on potential threats and set a balance between transaction costs and security level.

To find more about Starknet architecture, refer to the [ZK Rollups Landscape report](#) (page 29).

## EVM-Compatibility and Privacy

- **StarkNet zkVM and Cairo 1.0**

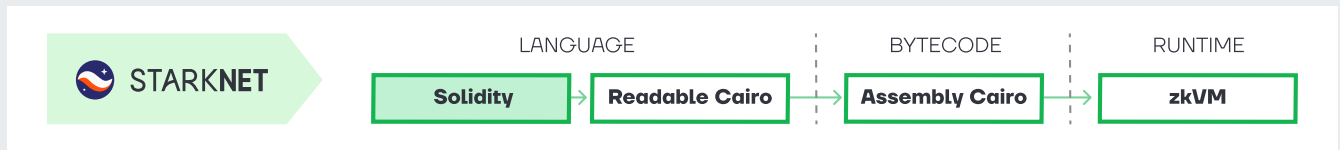


Figure 15. StarkNet zkVM.

Source: zkValidator: “zkEVMs Beyond Polygon and zkSync”.

The Cairo VM is a zkVM optimized for zero-knowledge proofs, making it simpler to construct and offering enhanced flexibility. It is also more cost-effective to optimize circuits and Provers for a zkVM compared to developing a zkEVM. The memory model in Cairo VM is write-once.

The Cairo VM, known for its cost-effective computation, enables the running of machine learning models, although it doesn't have native features specifically for AI or ML. This VM is specially designed for Validity Proofs and is not compatible with EVM. While the use of Rust eases the onboarding process for new developers, mastering Cairo can still be challenging, particularly considering the limited pool of Web3 developers.

Starknet ecosystem, which is currently undergoing a lot of fundamental changes due to the release of Cairo 1.0 and compatible Starknet contracts.

- **Kakarot zkEVM**

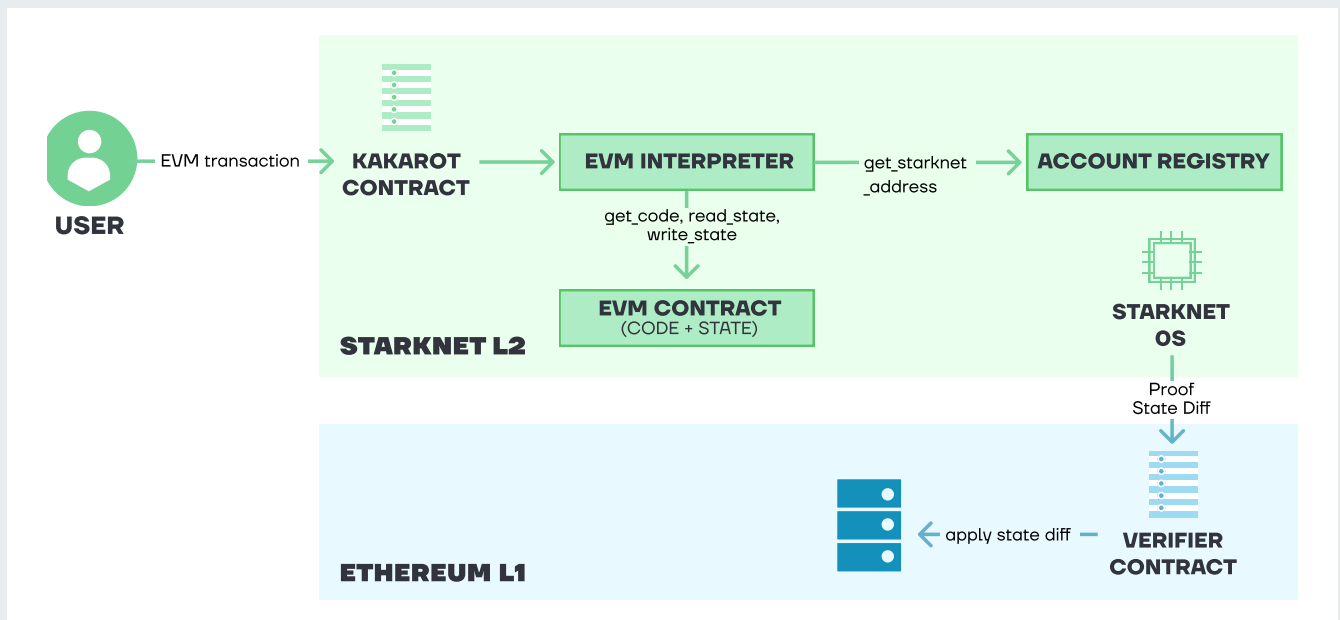


Figure 16. Kakarot zkEVM.

Source: Starknet Book.

However, in 2023, Starknet showed the process of transitioning from Type 4 to Type 3/Type 2.5 zkEVM, which is nearly EVM-equivalent. While Type 2.5 may temporarily omit a few EVM features and have possible risks around gas setting and compatibility, it serves as a logical precursor to achieving Type 2, which will be fully EVM-equivalent.

Kakarot, operating on Starknet's Goerli testnet, is a Cairo-based smart contract abstraction layer that doubles as an EVM bytecode interpreter. It enables users to execute EVM bytecode, deploy EVM smart contracts, and interact with their functions. Remarkably, Kakarot has implemented 100% of EVM opcodes and 8 out of 9 EVM precompiles, and is progressing towards its testnet launch. Its codebase is significantly smaller than the average zkEVM codebases. However, it's important to note that Kakarot currently lacks native Account Abstraction functionality, largely due to Ethereum itself not having AA functionality.

“



**Danilo Kim**  
Co-founder



**Kakarot**

Kakarot is an (zk)-Ethereum Virtual Machine implementation written in Cairo. Kakarot is Ethereum compatible, i.e. all existing smart contracts, developer tools and wallets work out-of-the-box on Kakarot.

Kakarot is a Type 2.5 ZkEVM written in Cairo, a Turing-complete programming language. Cairo 0 is designed to compile into Cairo Assembly(CASM), which generates execution traces. These traces are then used to produce Stark Proofs.

Kakarot originated in October 2022 as a community initiative during a StarkNet Hacker House. Since then, it has evolved into a company with the mission of scaling Ethereum.

Thanks to robust and vivid community engagement and the capabilities of Cairo, developed by the Starkware team, Kakarot achieved full opcode equivalence in just two and a half months. We are currently in the process of launching our first testnet, which will function either as an L2 on Ethereum.

Beyond this initial stage, we plan to become a Type 1 ZkEVM, which will enable any L1 node to generate Stark Proofs. Additionally, we are currently exploring other ZKPs, account abstraction, and scaling solutions that can contribute to the growth and resilience of the Web3 space.

”

- **StarkEx for privacy**

With the flexible settings of the latest version of StarkEx, you can create private solutions on L3/L4 that do not publish data off-chain, ensuring complete data confidentiality. However, this approach may potentially impact user security in the event of Operator exploits or other failures in the main network of the private solution.

Off-chain data storage appears to be the optimal choice, particularly when considering privacy aspects in the context of SNARK-based Layer 3 solutions settling on Layer 2. Some solutions, such as the cryptographic and pairing library Garaga, are actively developing features to enhance privacy within Starknet.

# Ecosystem

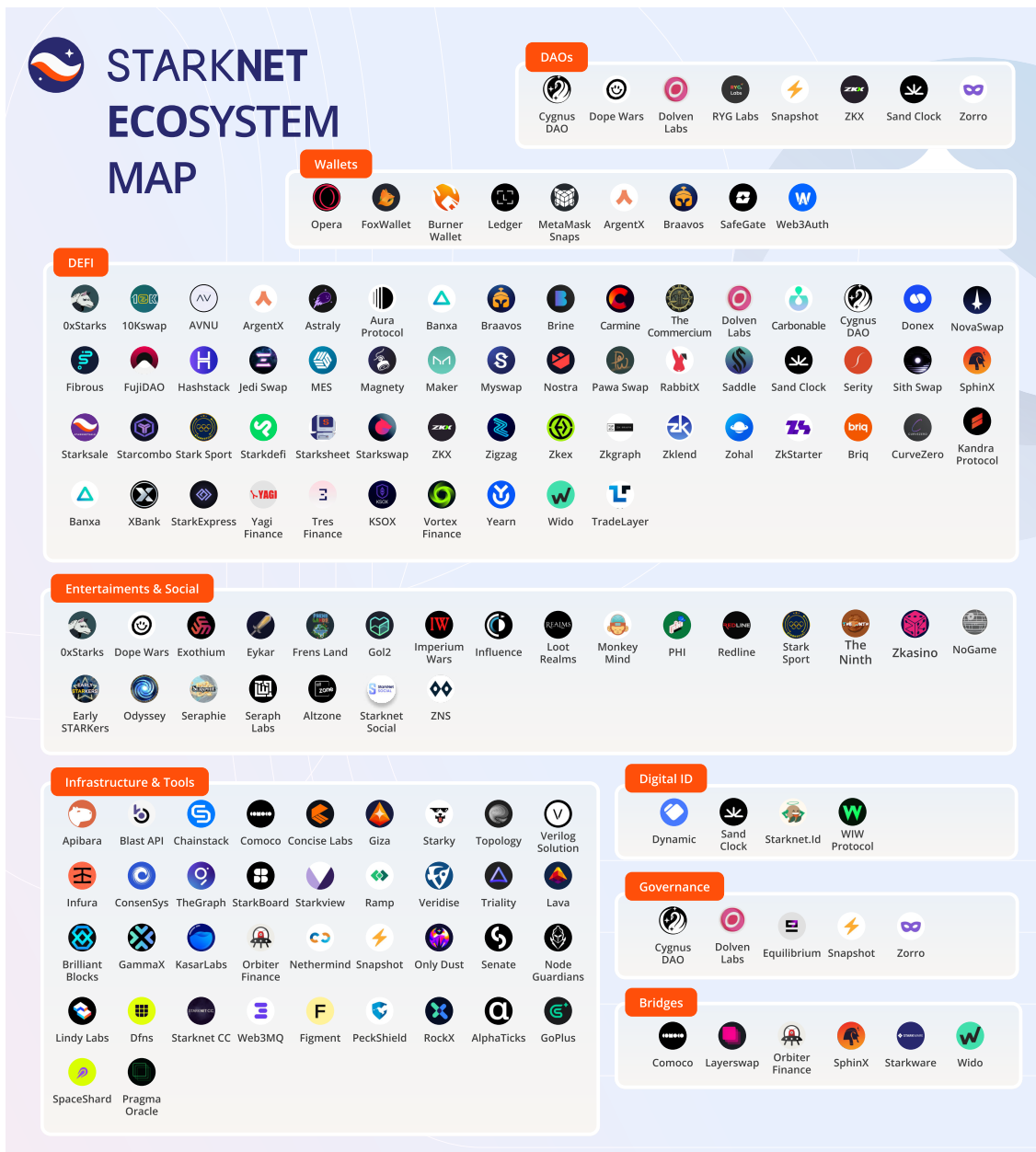


Figure 17. Starknet Ecosystem.

Source: Cryptomeria Capital.

## Roadmap

- **March 2023** - Testnet for transition to Cairo launch
- **April 2023** - Mainnet launch

### Next notable developments include:

- The closest update is going to be added on 18th **December 2023**. As part of such a version, on the way to improving the work of the Sequencer and reducing its centralization, the Starknet feeder gateway will be completely disabled.

- Kakarot zkEVM Mainnet launch
- Network stability improvements
- Fixed and short block intervals
- Fee market of transactions
- A reduction in transaction costs via Volition

## Conclusion

Starknet, operating as a Validity Rollup, has strategically incorporated the Cairo VM with the STARK proof system to optimize the efficiency of Validity proofs. It presents a modern vision of transactional processes with statuses like "submitted", "accepted on L2", and "accepted on L1", which integrate off-chain security with Ethereum's L1 security. The network uniquely endorses Account Abstraction (AA), transforming all accounts into smart accounts. This advanced integration paves the way for initiatives such as Visa's exploration of "auto payments for self-custodial wallets", leveraging StarkNet's AA capabilities.

StarkEx stands out as a self-custodial scalability engine, allowing dApps to deploy an auxiliary infrastructure layer that can operate as either a separate Rollup or Validium. Its Volition protocol offers users the flexibility of on-chain and off-chain data storage, and with Data Availability Committee (DAC), there's a provision for off-chain data storage with enhanced privacy through encryption. Starknet also offers multi-layer scaling through shared DA levels and seamless L1 <-> L2 messaging. In tandem with scaling, Starknet's approach with zk-STARKs, utilizing the FRI polynomial commitment scheme, promotes off-chain computation, ensuring reduced Mainnet workload and lower transaction costs.

While Starknet currently operates with CairoVM, there's an ongoing transition towards being EVM-compatible with the introduction of Kakarot zkEVM. Kakarot, still in its test phase, promises the execution of EVM bytecode and deployment of EVM contracts. This movement from Type 4 to nearly EVM-equivalent Type 2.5 zkEVM showcases Starknet's commitment to progress and adaptability. Moreover, with privacy becoming a pivotal focus, StarkEx's potential to create private solutions on L3/L4 without off-chain data publishing symbolizes a balance between privacy and user security.



**Edi Sinovčić**  
Founder and CEO

### SPACE SHARD

SpaceShard is a full-cycle blockchain development company —with its own R&D department — that is focusing on Zero-Knowledge Proof technology within the Starkware ecosystem.

We see more and more maturity on the zk non-privacy stack, where there is a plethora of solutions that offer blockspace. both on zkEVM and zkVM side.

Who will use all of that blockspace? While short term it seems that there are no users and there is no real need for all of that, it will soon become clear (as macro becomes better) that there will be instant demand for it. One of the biggest hurdles that still persist is interoperability. It feels like Ethereum sharding roadmap reimplemented but with rollups now, without much standardization on the way.

It will be interesting to follow progress on zk rollups (especially private ones) and how they tackle both technical challenges of decentralizing the network on start and navigating regulatory challenges along the way.

One of the biggest problems that we see and are trying to solve with Nimborra is how do we use all this zk power to scale Ethereum without bringing more hurdles for the users, so we can abstract chains, wallets etc.



## Introduction

Scroll is a ZK rollup that is promising a true EVM-equivalent execution environment. One of the main features being worked on by the Scroll team is parallelizable proofs, so that the Prover market is less of a winner-take-all and a more energy efficient, meritocratic architecture.

The Scroll team has been very closely working with Ethereum’s privacy and scaling group to develop their system. Because it is intended to be strictly EVM-equivalent, account abstraction is not natively supported by scroll.

Scroll aims to enable the verification of an Ethereum block using a single, concise proof. This method focuses on ensuring the consistency and accuracy of each operation in the EVM execution process. With such an approach, L1 smart contracts can be easily transitioned to Scroll. Instead of introducing new techniques, the existing EVM will be enhanced through tailored optimizations. This ensures compatibility with current Ethereum systems without necessitating any alterations.

## Architecture and Fundamental Components

Below you can see a quick overview of Scroll Architecture.

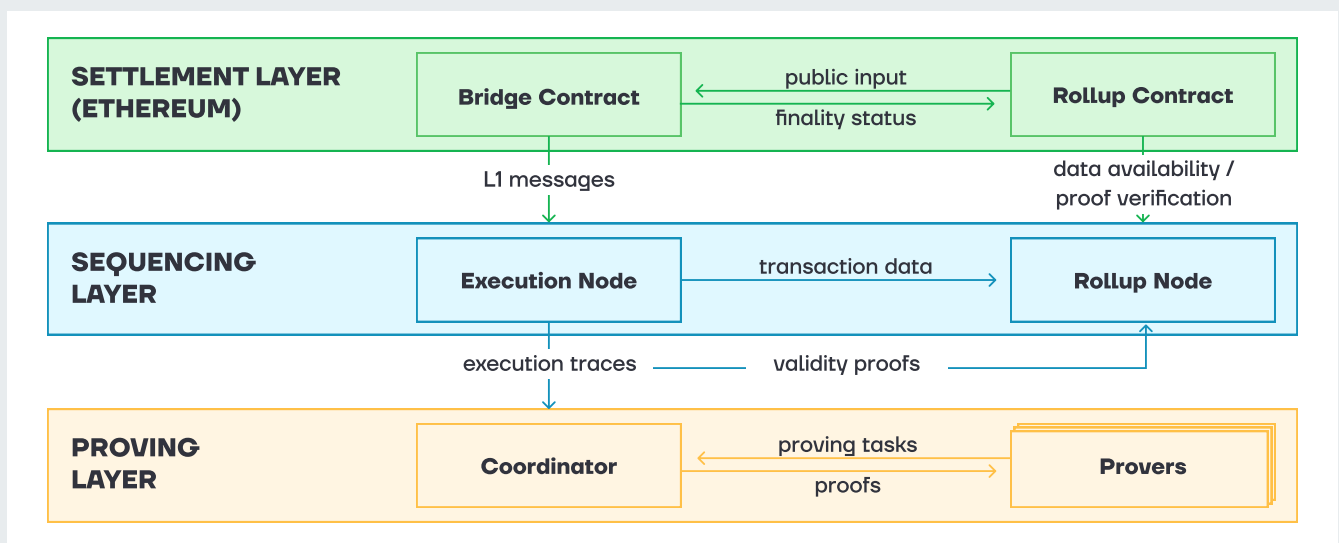


Figure 18. Scroll High Level Architecture.

Source: Scroll Documentation.

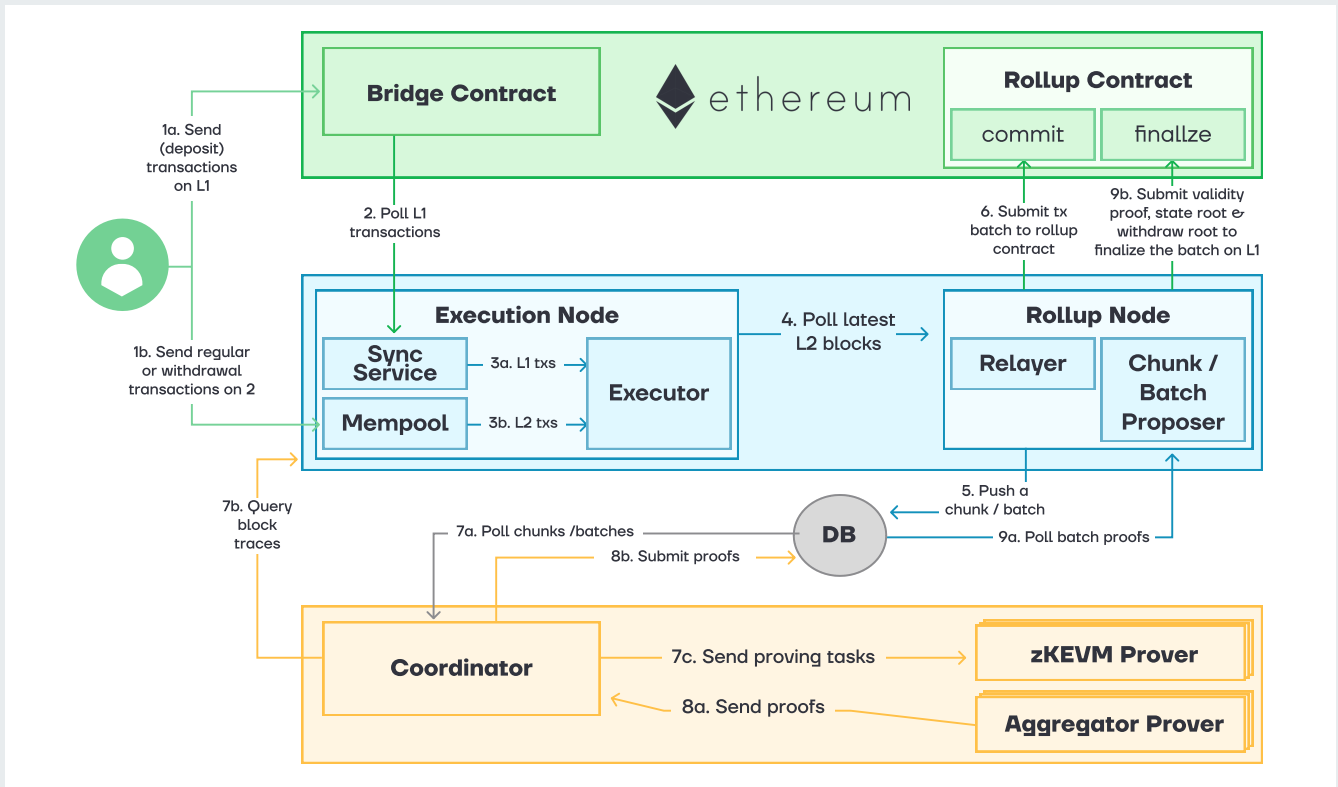


Figure 19. Scroll Detailed Architecture.

Source: Scroll Documentation.

- **Modified version of ZCash’s “Halo2” code**

One of Scroll’s key differentiators is its use of a modified version of ZCash’s “Halo2” code, which allows protocols to harness the benefits of SNARKs’ small proof size and quick proof verification, while removing the need for a trusted setup – the Achilles’ heel of SNARKs. They have modified Halo 2 to use KZG as its polynomial commitment scheme (rather than its default scheme, IPA) in order to achieve more efficient on-chain proof verification.

Proof generation unfolds in three phases. First, a "witness" is created. This witness, also termed the "trace," offers data supporting a statement's truth. In the context of the Square-Fibonacci, it's a sequential computation presented in a table, demonstrating mathematical relations of the sequence.

The second step focuses on committing to this witness. Here, the witness is compressed into a concise representation. A polynomial commitment scheme is used, allowing for validation of original witness properties using only its compressed form.

Lastly, the validity of the witness is checked. The generated witness must comply with set criteria. In the Square-Fibonacci case, the computations must match the Fibonacci sequence’s mathematical equation. A compact proof of the witness's adherence is then generated. For proof validation, only the compressed witness from the second step is needed. Grasping these steps in detail requires understanding polynomial principles.

- **The Roller Network and Performance Optimization**

The Scroll Network employs a decentralized group of Provers, known as the Roller network. This group aids in creating proofs for the Scroll's second-layer blocks. This encourages not only the expansion of hardware capabilities but also the development of a diverse and evolving digital environment.



To enhance efficiency and decrease on-chain verification expenses, Scroll uses a special aggregation circuit. This circuit takes multiple proofs and consolidates them into a single, streamlined proof. This process aids in significantly reducing the computational and cost overhead usually associated with verifying numerous proofs.

Also, Scroll has incorporated an optimized GPU Prover via the implementation of different kernels, overlapping CPU and GPU computation, and memory optimization for faster core computation.

- **zkTrie**

Scroll replaced the Patricia Merkle Trie by a more zk-friendly data structure, called zkTrie, for both state trie and storage trie. In the high level, the zkTrie data structure is a sparse binary Merkle tree that is used to store key-value pairs efficiently with the Poseidon hash, a zk-friendly hash function.

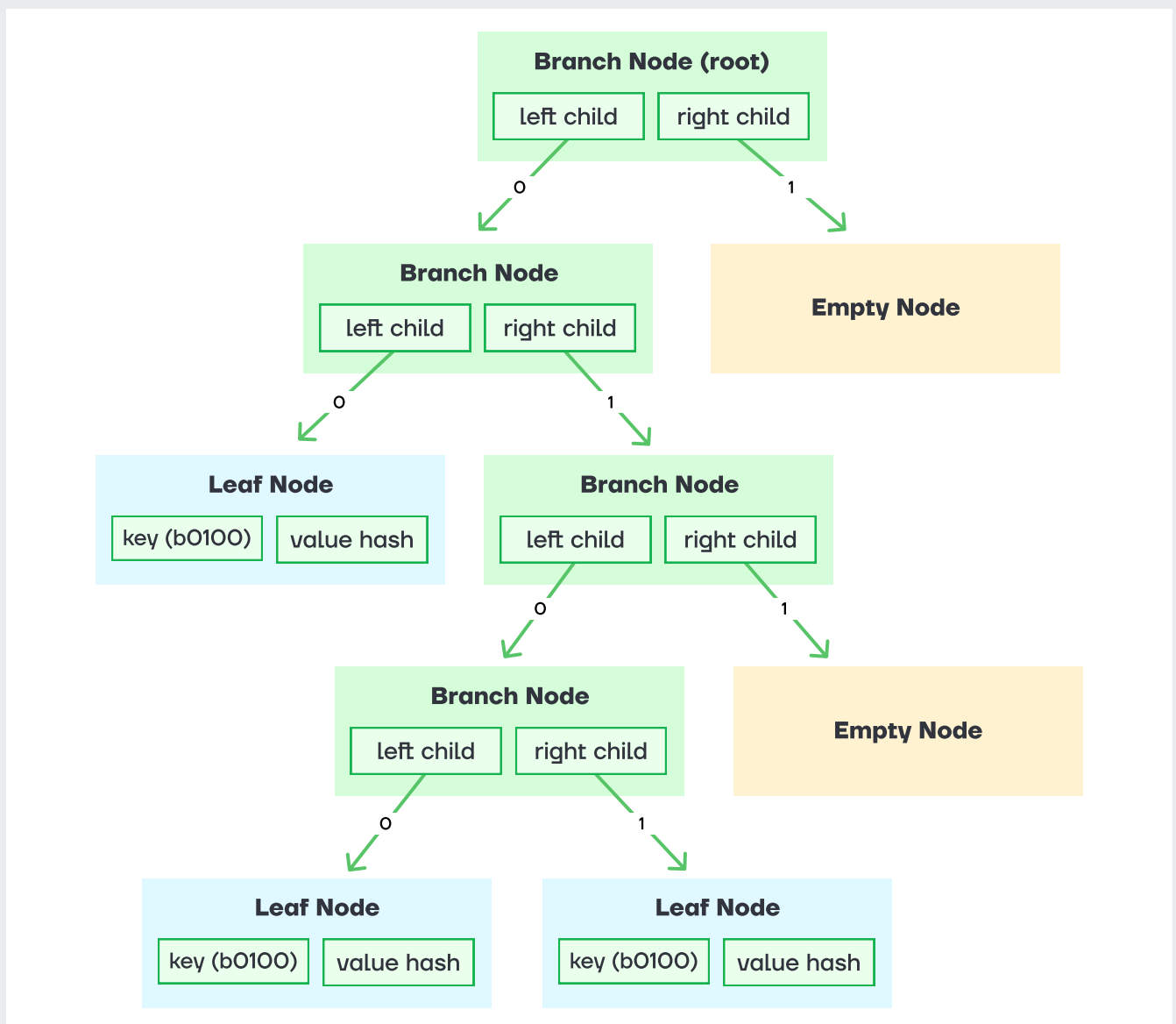


Figure 20. zkTrie.

Source: Scroll Tech Documentation.

- 1. Secure Key Creation:** To start, a unique and consistent key is generated for the data's storage location. This is done by hashing the original key (which might be an account address or storage key) using a cryptographic method known as the Poseidon hash function. The resulting "secure key" is spread evenly across the possible storage spaces, ensuring a balanced distribution.
- 2. Path Encoding:** The exact location, or path, where the data will be stored is determined by examining the secure key bit by bit, starting from the least significant and ending at the most significant. For each bit in this key, if it's a '0', the path moves to the left branch in the tree, and if it's a '1', it moves to the right.
- 3. Depth Limitation:** The depth (or how deep the data can be stored in the tree) of zkTrie is capped at 248 levels. This is because while the Poseidon hash creates keys that could theoretically be spread over  $2^{256}$  different locations, in practice, it doesn't fill this entire range. Using the entire 256-bit length could lead to ambiguities, which in turn might result in errors in the zero-knowledge proof system. By only considering the first 248 bits, this ambiguity is avoided.
- 4. Depth Optimization:** For efficiency, any subtree that only holds a single piece of data (or leaf node) is simplified down to just that data point. As an example, consider a tree diagram where you have three distinct keys: 0100, 0010, and 1010. The data for the key 0100 doesn't expand fully to the depth it could because it shares a common feature (the ending '00') with no other key, thus saving space.

To find more about Scroll architecture, refer to the [ZK Rollups Landscape report](#) (page 36).

## EVM Compatibility and Privacy

### • Scroll zkEVM

Scroll is working towards EVM equivalence to ensure full compliance with the EVM specification, offering an implementation close to that of Ethereum. This approach aids in enhancing security by reusing numerous Ethereum stacks. Currently it's a Type 3 zkEVM with some improvements that move Scroll to Type 2.



Figure 21. Scroll zkEVM.

Source: zkValidator: "zkEVMs Beyond Polygon and zkSync".

Scroll's zkEVM introduces some modifications when compared to the traditional Ethereum setup. Notably, the zkEVM currently omits support for SHA2-256, RIPEMD-160, and blake2f precompiles, but plans to incorporate them in an impending hard fork. The modexp precompile and ecPairing precompile in zkEVM have been adjusted to support smaller inputs and a limited number of points, respectively. The platform also presents a unique StateAccount object, featuring the additions of PoseidonCodehash and CodeSize. Contracts in Scroll hold dual codehash types - Keccak for compatibility and Poseidon for efficiency. To streamline EXTCODESIZE verification, Scroll pre-stores the contract size during its creation. Furthermore, the Sepolia Testnet targets a swift 3-second block time, a significant improvement over Ethereum's approximate 12-second interval. For smart contract compilation, the "London" version is endorsed. Transaction fees in Scroll Sepolia have a dual structure, consisting of L2 gas fees and L1 data fees, the latter applying only to L2-initiated transactions. Lastly, Scroll remains attentive to new Ethereum EIPs, integrating them as deemed fit.

Scroll is taking a longer road by design by building “at the bytecode level” in order to “behave exactly like the Ethereum Virtual Machine” in every way possible. Bytecode is the machine-readable form of code that dictates precisely how a program is to execute.

Related to this, Scroll maintains two types of codehash for each contract bytecode: Keccak hash and Poseidon hash. KeccakCodeHash is kept to maintain compatibility for EXTCODEHASH.

PoseidonCodeHash is used for verifying correctness of bytecodes loaded in the zKEVM, where Poseidon hashing is far more efficient.

## Ecosystem

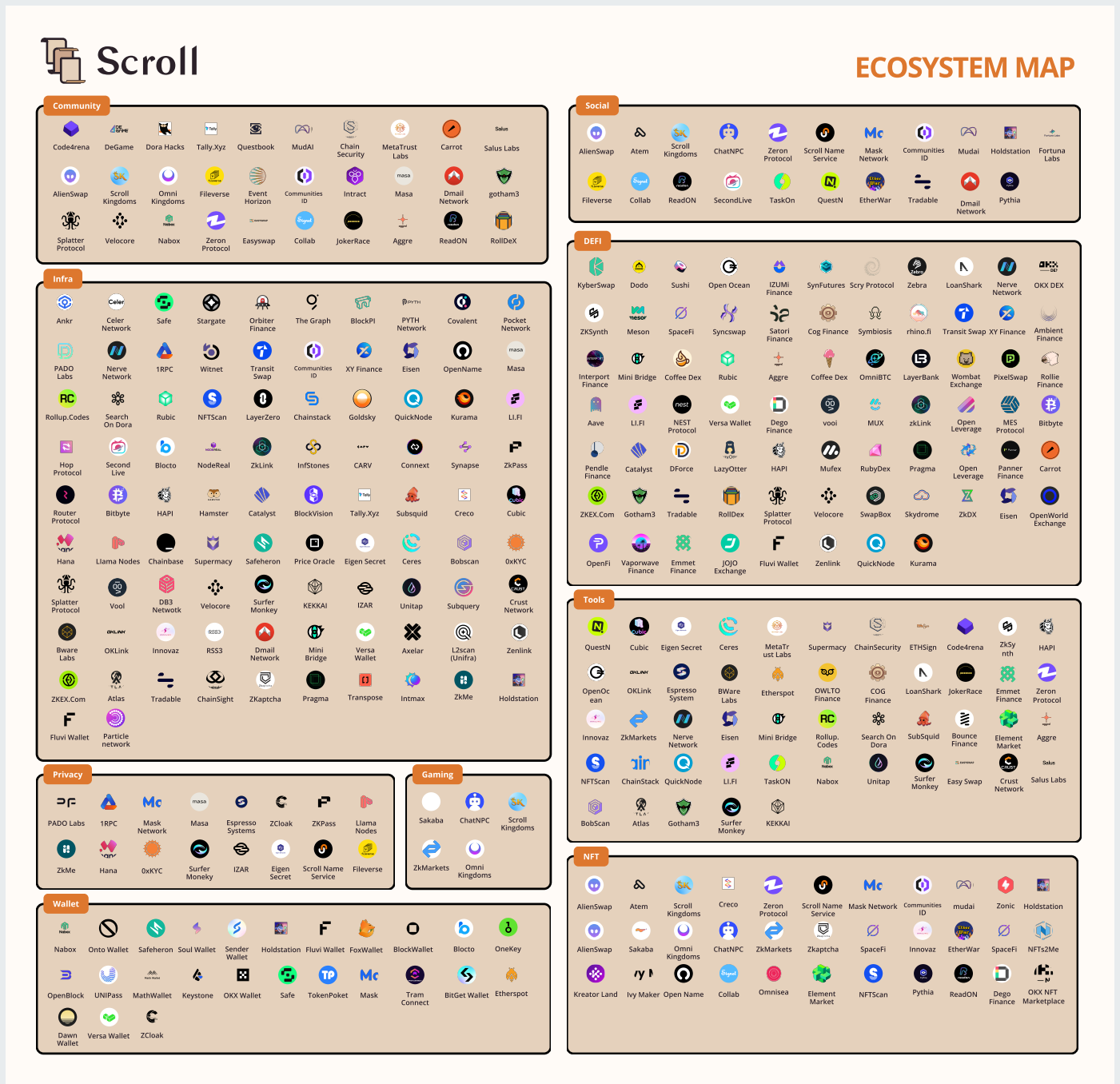


Figure 22. Scroll Ecosystem.  
Source: Scroll - Ecosystem.

## Roadmap

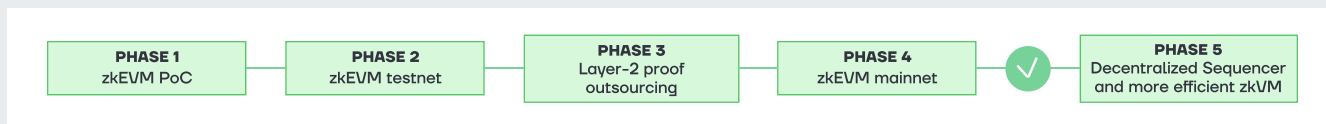


Figure 23. Scroll roadmap.

Source: Scroll Documentation.

- **September 2021** - zkEVM creation.
- **July 2022** - Pre-Alpha testnet launch.
- **October 2022** - first big network update. Support the ERC-20, ERC-721, and ERC-1155 standards. Hardhat and Foundry became possible to use.
- **January 2023** - update "O109". Aggregated blocks, hosting separation, security updates, etc.
- **July 2023** - contributing program announced.
- **October 2023** - mainnet launch.

### Next notable developments include:

- Establishing a security council
- Collaborating with the community to implement various Sequencers
- Adding SGX Prover

## Conclusion

Scroll is a ZK rollup designed to replicate the Ethereum EVM, emphasizing compatibility and optimized performance. By enhancing the existing EVM rather than devising entirely new methods, it seeks to ensure seamless integration of L1 smart contracts. Scroll employs a modified ZCash's Halo2 code with the KZG polynomial commitment scheme for efficient on-chain proof verification. It also features the decentralized Roller Network for proof generation, and the zkTrie data structure, a zk-friendly Merkle tree, to efficiently store key-value pairs using the Poseidon hash function. While aligning closely with Ethereum's EVM, Scroll has distinct features like select precompile support, additional state account fields, dual codehash types, and a unique fee structure. It balances adherence to Ethereum's standards with its own tailored optimizations to achieve its goals.

In March 2023, Scroll announced a successful \$50M fundraising round at a \$1.8B valuation. And, in October, they successfully launched the Scroll zkEVM mainnet, according to blockchain data.



**Shahryar Hasnani**  
Partnerships



Scroll is the community-first, native zkEVM built upon Ethereum—designed for scaling without sacrificing security, developer, or user experience.

From its inception, Scroll has been rooted in the belief that Ethereum's ethos of decentralization and credible neutrality are critical to the future of blockchain—and that the innovation of zero-knowledge proof technology is the next step in unlocking that potential. By building an EVM-equivalent, bytecode-compatible zkEVM, we're not only enhancing scalability and security, but also paving the way for a better developer and user experience.

The first and most prominent use case for ZK is compression and scalability; this is considered to be the endgame for scaling Ethereum and bringing on the next wave of users, and is the core way Scroll leverages it. ZK scaling is trustless, verifiable, and has compounding effects. As such, it solves for Ethereum's throughput challenges without sacrificing its lightweight node requirements, and it also extends to practically any other blockchain architecture. It is still in its early phase, but beyond Layer 2s, several Layer 1 blockchains are also experimenting with and adopting ZK to scale, and we can expect many more in the future.

The other prevalent ZK use case is privacy. The ability to validate transactions without revealing their content enables an entirely new paradigm of blockchain interaction. This allows people to transact, get paid, communicate, vote, and prove their reputation without having to reveal private information; these are all critical rights in the real-world that are in high demand in crypto. Again, this use case is being implemented at the Layer 1 and Layer 2 level, as well as directly at the application level. ZK privacy faces a more uncertain regulatory path, but will undoubtedly become a mainstay in the industry over the long-term.

Beyond scaling, ZK offers several other nascent applications, namely verifiable computation and trustless bridging and messaging. Verifiable computation allows blockchains to offload data-heavy work without making any risky assumptions about the results; this enriches applications and smart contracts to a level previously only available outside of crypto. Bridging and messaging are a hotspot for exploits due to the various trust and security assumptions associated; ZK tech enables the fastest trustless method to message across chains, and various teams are working on extending this advantage to cross-chain asset transfers and more.

As the need for scalability and security becomes even more pronounced, we stand by our conviction that ZK technology is the critical catalyst for the blockchain industry—to become safer, more user friendly, and more transformative for the world.



## THE FUTURE OF ZKP

“

The potential of zero-knowledge proofs (ZKPs) in reshaping the digital landscape, especially in the context of Web3 and beyond, is significant and is currently being explored in the Web3 and conventional world as well.

In the Web3 and Blockchain world, ZKP has significant advantages. ZKPs allow for the verification of information without revealing the information itself. This is crucial for Web3 applications where user privacy and data security are paramount. ZK-rollup technology uses ZKPs to aggregate multiple transactions into a single proof. This significantly reduces the amount of data stored on the blockchain, enhancing scalability and performance. In addition, ZKPs can enable private transactions and smart contracts on public blockchains, allowing for more complex and sensitive financial, legal, and business activities to be conducted securely.

In the Conventional Business and Industry Sectors there are several use cases being explored. In banking and finance, ZKPs can streamline KYC (Know Your Customer) and AML (Anti-Money Laundering) processes while preserving customer privacy. They could enable the validation of financial transactions and credentials without exposing sensitive data. Similarly, Patient privacy is a critical concern in healthcare. ZKPs could allow for the secure sharing of medical records and personal health information, ensuring compliance with regulations like HIPAA while facilitating research and treatment.

For Supply Chain Management, Voting Systems, Entertainment and Media there are innumerable use cases being explored. ZKPs facilitate secure data sharing between organizations without exposing proprietary information, fostering collaboration and joint ventures. This could be one of the most important use cases for companies who are struggling to cross-collaborate within the organization. The ZK cryptographic method has the capacity to transform conventional businesses, influencing major industries by enhancing security, streamlining compliance processes, improving customer privacy and cross-organizational collaboration, Zero-knowledge proofs will provide businesses across a variety of sectors with the means to achieve greater efficiency, trust, and innovation.

In the years to come, this technology will emerge as a strategic resource to solve the significant challenges. It will play a crucial role in facilitating the next generation of applications by achieving increased performance through ZK-rollup technology and introducing a privacy layer to Web3. As the landscape of Zero-knowledge proof technologies continues to mature and evolve, its benefits and use-cases are likely to broaden, significantly reshaping the future of digital transactions.

Several challenges remain as implementing ZKPs is technically complex and resource-intensive. There's a need for more user-friendly tools and platforms to facilitate widespread adoption. As with any emerging technology, navigating the regulatory landscape will be crucial. Ensuring compliance with data protection laws and other regulations will be essential. There is also a significant educational gap that needs to be bridged to enable broader understanding of the adoption of ZKPs.

As the ecosystem continues to evolve, the applications of ZKPs are expected to become more diverse and integrated into various aspects of digital transactions and beyond. The technology is poised to play a key role in achieving a balance between privacy and transparency, a cornerstone in the trustless environments of Web3 and the modern digital world

We are pleased that organizations such as Cryptomeria have seen ZKP as the technology to bet on to solve the myriads of problems faced in the increasingly digital world. At Arthur D Little, we believe that new technologies should be given the time and space to evolve and establish themselves. While there is no guarantee of success, the outcome of not fostering new and novel technologies is always zero.



## **FEROZ SANULLA**

Partner, Arthur D Little  
Head of Technology and Innovation MEI

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information please visit [www.adlittle.com](http://www.adlittle.com) or [www.adl.com](http://www.adl.com).

Copyright Arthur D. Little Luxembourg S.A. 2022.

## Introduction

Aztec is a fully programmable private smart contract platform built as a Layer 2 network on Ethereum.

Aztec is designed to help build and deploy private smart contracts with features like private functions, private persistent state, private bytecode, private contract composability, encrypted state transitions, and encrypted logs, while retaining composability with Ethereum L1.

Aztec is being built by Aztec Labs, the core contributors of the Noir zkDSL, which is intended to make writing zero knowledge circuits easier. While Noir can be used in any EVM-compatible context, Aztec.nr is a framework for writing Aztec smart contracts, written in Noir.

## Fundamental Components

- **UTXO model**

Aztec uses a UTXO model, similar to Bitcoin and zCash, to prioritize user privacy. Its core difference from other blockchains is its reliance on zero-knowledge proofs to validate transactions, as opposed to transaction requests. This design aims to combine the privacy benefits of UTXO models with the application flexibility of platforms like Ethereum.

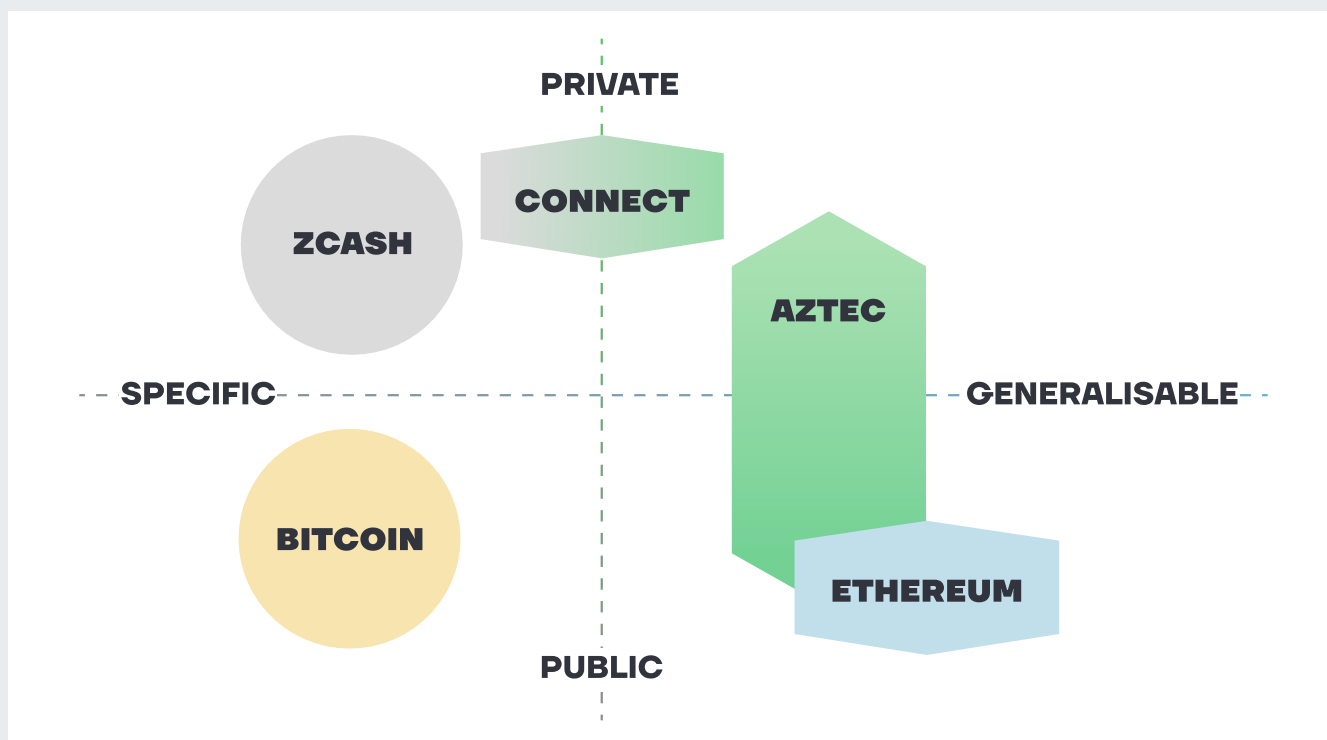


Figure 24. Aztec Competitor Overview.

Source: Aztec: the Hybrid zkRollup.

- **Noir Circuits**

In Aztec, the design of smart contracts is not based on the EVM or Solidity frameworks. Instead, they consist of Noir Circuits that define both public and private functions. These functions interact with data



states held by the contract. The representation of each function is through ZK SNARK verification keys. The network has two primary Circuits, termed as public and private kernels, which validate the execution of these function calls. Transactions are formed by producing proofs for these kernels in an iterative manner, managed through FIFO queues and split into two distinct categories for public and private calls.

A Sequencer oversees the order of these calls, ensuring the accurate processing of transactions. Private function calls are processed first, with users submitting their proofs. Public functions, which can change the system's state, are then processed. If any part of a transaction fails, it is entirely discarded to maintain system integrity. The Sequencer's role is pivotal in maintaining order and ensuring that all functions are executed correctly.

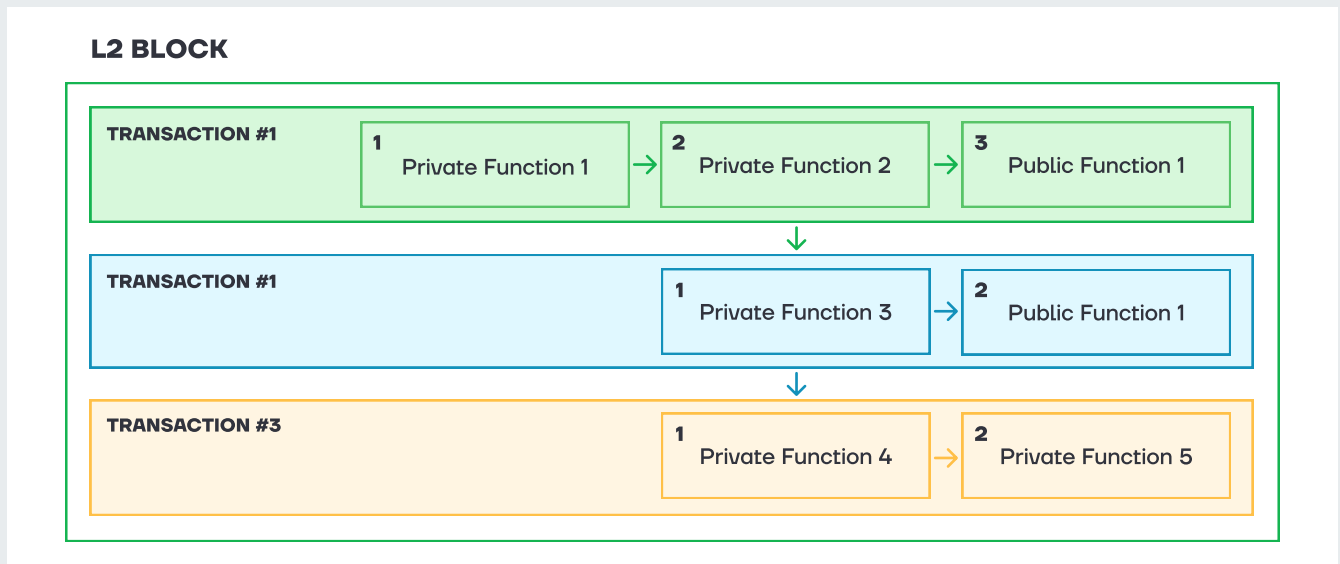


Figure 25. Transaction Ordering.  
Source: Aztec Documentation.

To find more about Aztec architecture, refer to the [ZK Rollups Landscape report](#) (page 41).

## EVM-Compatibility and Privacy

- Aztec zkVM

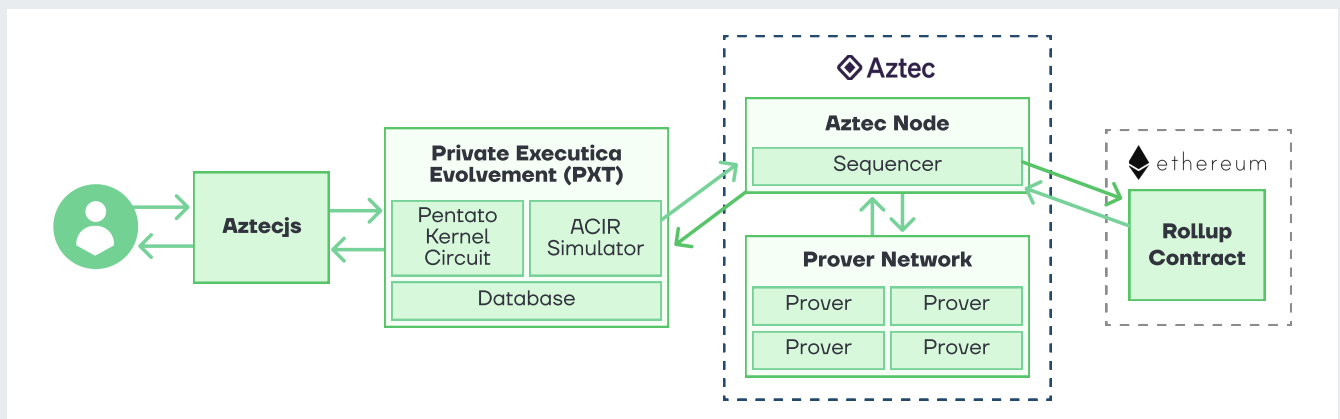


Figure 26. High level network architecture.  
Source: Aztec Documentation.

The main narrative of Aztec is that privacy can't be EVM-Compatible. Aztec's architecture is distinct from the traditional EVM design. This divergence stems from Aztec's prioritization of user privacy, resulting in an inherent tension with standard EVM constructs and Solidity's semantics. While Ethereum relies on a transparent, account-based model, Aztec merges the UTXO approach with elements of public smart contract platforms, creating a unique hybrid zkRollup system.

Aztec's encryption utilizes zero-knowledge proofs and homomorphic encryption to maintain transaction privacy while preserving integrity. Inputs and outputs of a transaction are encrypted, yet the network, using these methods, can verify the transaction's logical correctness without exposing its specific details. Homomorphic encryption enables operations on encrypted data, providing results as if operations were on the original data, ensuring the blockchain can validate encrypted statements without accessing the underlying values.

## Ecosystem

In the earlier iteration, Aztec Connect facilitated the deposit of funds into multiple DeFi protocols, including LiDo, Element.Fi, and others. Users were able to deposit funds into the Aztec Connect contract through various interfaces, such as zk.money and other front-ends like zkpay.finance.

Currently, the Aztec Ecosystem is still in its initial phase of development, with new projects emerging that utilize the Noir codebase.

## Roadmap

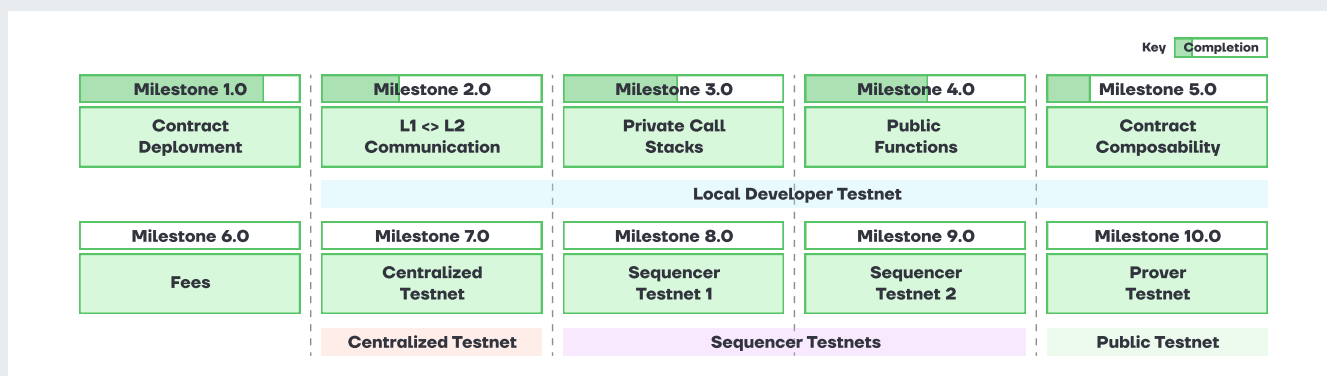


Figure 27. Aztec roadmap.

Source: Aztec: "the Hybrid zkRollup" OR Aztec Documentation.

- 1: Development Strategy
- 2: L1-L2 Communication
- 3: Private call stacks
- 4: Public Functions
- 5: More Composability
- 6: Introducing fees
- 7: Introduce actual circuits, proofs and Verifiers
- 8: Public testnet via a centralised Sequencer
- 9: 1st Sequencer testnet
- 10: 2nd Sequencer testnet
- 11: Prover testnet
- 12: Refactoring / Optimisations

## Conclusion

Aztec is a zk-zkRollup that employs two layers of Zero Knowledge Circuits. The first layer is purposed for encrypting user transactions, while the second is for compressing these transactions to optimize validation processes. Instead of following the design patterns of common blockchains, Aztec implements a UTXO model, reminiscent of structures observed in Bitcoin and zCash. Bypassing the EVM and Solidity frameworks, its smart contracts are constructed using Noir Circuits. These circuits, which have both public and private functionalities, utilize ZK SNARK verification keys for representation. The network processes transaction proofs sequentially, with a designated Sequencer ensuring the chronological processing of transactions. Aztec's structural design suggests that obtaining privacy might be challenging within the scope of EVM compatibility. The architecture, differing from standard EVM and Solidity designs, integrates the UTXO model's privacy attributes with characteristics common to public smart contract systems, thus developing a specific type of zkRollup system. Through this design, while the specifics of a transaction are encrypted, their correctness can be validated using zero-knowledge proofs in conjunction with homomorphic encryption. In its earlier version, Aztec Connect permitted interactions with several DeFi Protocols, enabling deposits from interfaces such as zk.money and zkpay.finance. Currently, the Aztec system is undergoing development, introducing tools like [Aztec.nr](#) for private state management, Fernet that utilizes a leader election mechanism, and BattleZips, a game that utilizes zero-knowledge proofs in its mechanics.

## Introduction

Polygon zkEVM is a decentralized Ethereum Layer 2 scalability solution that uses cryptographic zero-knowledge proofs to offer validity and quick finality to off-chain transaction computation.

## Architecture and Fundamental Components

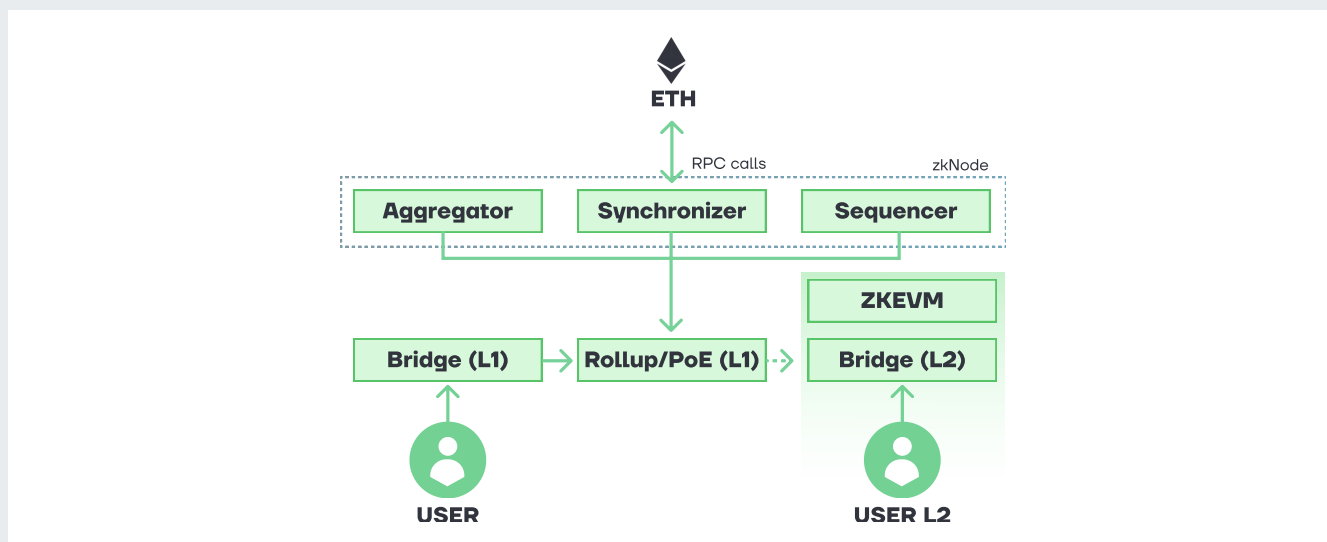


Figure 28. Skeletal Architecture of Polygon zkEVM.

Source: Polygon Wiki: "zkEVM".

### • Consensus Contract (PolygonZkEVM.sol)

Polygon's zkEVM manages state changes from Ethereum Layer 2 transactions and produces validity proofs using zero-knowledge methods to verify these adjustments.

The updated zkEVM Consensus Contract, deployed on Layer 1, transitions towards a Proof of Efficiency approach, still drawing from the experiences of the PoD in v1.0, but emphasizing open participation for mainns in Layer 2 batch production.

The Consensus Contract model integrates the pre-existing PoD mechanism and accommodates unpermissioned coordinator involvement in generating L2 batches derived from L1 rolled-up transactions. The contract, PolygonZkEVM.sol, utilizes a streamlined approach, optimizing efficiency and addressing the complexities inherent in the PoD mechanism.

Key objectives of the contract-based consensus include:

1. Preserving unpermissioned batch production in L2.
2. Prioritizing efficiency for enhanced network performance.
3. Achieving a satisfactory level of decentralization.
4. Ensuring network security against potential threats, notably from validators.
5. Balancing validation efforts with the overall value of the network.

Considering on-chain data availability, a comprehensive ZK-Rollup schema necessitates the on-chain

publication of both user data (necessary for state reconstruction) and validity proofs (zero-knowledge proofs). Given Ethereum's structure, on-chain data publication is associated with gas expenditures, a limitation with L1, prompting deliberations over selecting either a comprehensive ZK-Rollup or a Hybrid schema.

In the context of a Hybrid schema, two configurations emerge:

1. Validium: Only the validity proofs are on-chain, with data storage being off-chain.
2. Volition: Certain transactions have both data and validity proofs on-chain, while for others, only the proofs are published on-chain.

The feasibility of a Hybrid schema is contingent upon factors such as the potential acceleration of the proving module, which could offset validation costs.

The zkEVM protocol uses a validity proof to validate state transitions. State transition compliance with established rules is overseen by the Consensus Contract (PolygonZkEVM.sol), which is deployed on L1.

A designated contract assesses the validity proofs, ensuring accurate state transition via zk-SNARK circuits. This mechanism involves two fundamental steps: grouping transactions and validating them.

Within the zkEVM structure, there are two roles: Sequencers and Aggregators. In this bifurcated system:

1. Sequencers are responsible for grouping transactions into batches and submitting them to the Consensus Contract on L1.
2. Aggregators evaluate the legitimacy of these transaction batches and supply validity proofs. Any Aggregator, operating in a permissionless environment, can present a proof verifying the integrity of the state transition calculations.

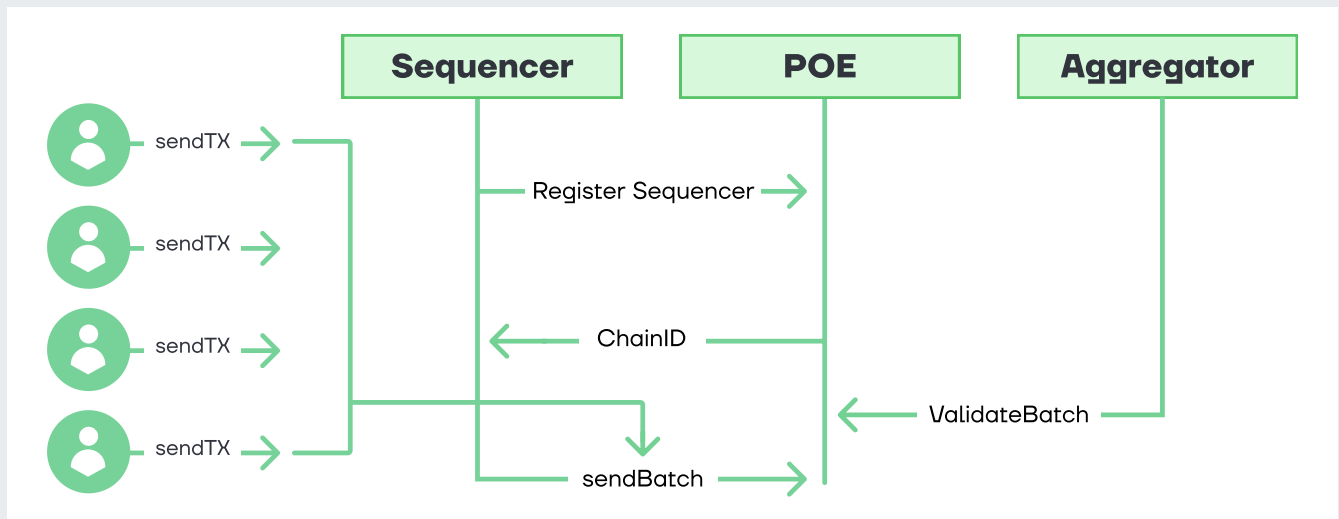


Figure 29. Sequencer and Aggregator operate within the smart-contract.

Source: Polygon Wiki: "zkEVM".

#### • zkNode

The zkNode software facilitates the operation of any zkEVM node, serving as a client for Synchronization and determining participant roles (either Sequencers or Aggregators). Participants in the Polygon zkEVM decide their mode of participation: as nodes to monitor network state or as actors in batch production, assuming the roles of Sequencer or Aggregator. The architecture of zkNode is designed with modularity.

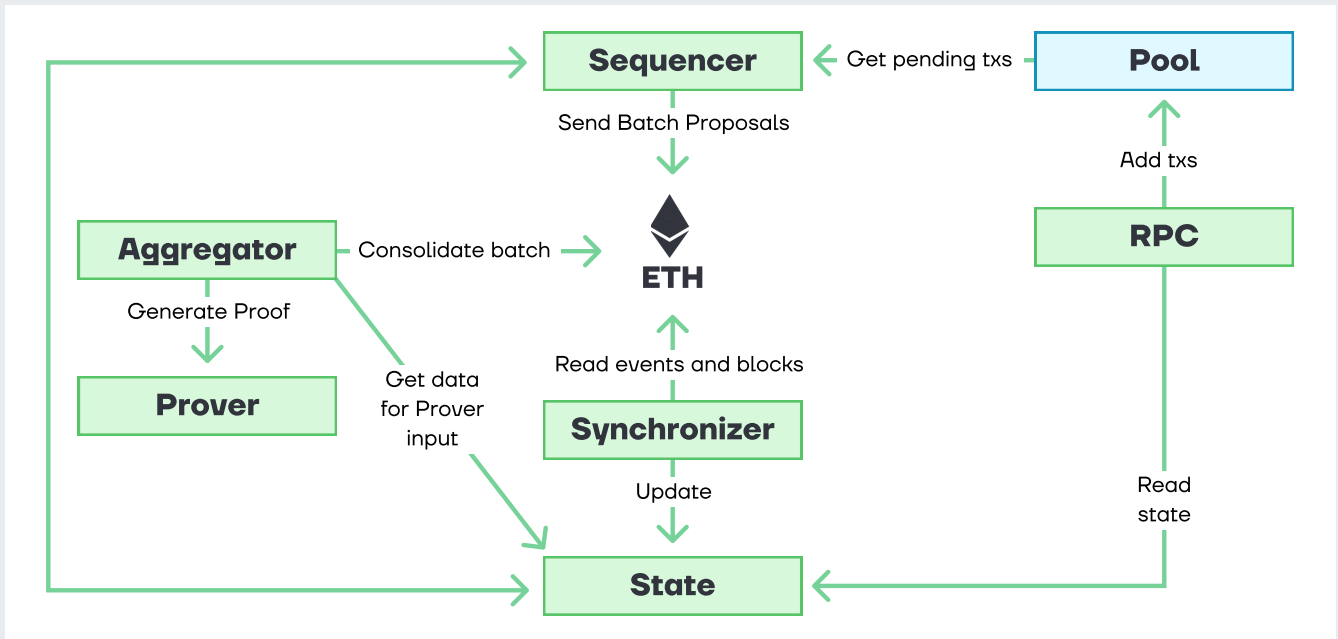


Figure 30. zkNode architecture.  
Source: Polygon Wiki: "zkEVM".

• **zkProver**

The zkEVM utilizes a specific zero-knowledge Prover (zkProver) to generate validity proofs. This prover is designed for server operations and aims for broad hardware compatibility. Within this framework, Aggregators employ the zkProver for batch validation and subsequent Validity Proof production. The zkProver integrates a primary State Machine Executor, supplementary State Machines, and proof-building components for both STARK and SNARK methodologies.

The zkEVM translates state modifications into polynomial representations, implying that each batch must adhere to polynomial constraints. In essence, the validation of batches relies on their compliance with these polynomial specifications.

The system comprises two distinct microprocessor-type state machines: Main SM and Storage SM. Both state machines possess firmware and hardware components, each with its distinct ROM. The firmware uses the zkASM language to detail logic and rules. These are saved in JSON format and subsequently interpreted by the specific SM Executor, which conducts storage actions as delineated in the JSON.

The hardware employs the Polynomial Identity Language (PIL) to specify constraints, saved similarly in JSON format. These constraints guide the specific SM Executor since all computations adhere to the polynomial identities.

Within the zkProver, two additional state machines focus on hashing: Keccak State Machine and POSEIDON State Machine.

The Keccak SM operates as a gates state machine, integrating logic gates and their interconnections. It's augmented by the Keccak SM Hash Generator and the Keccak PIL code, the latter ensuring validation.

The POSEIDON SM, modeled after the zk-STARK-friendly POSEIDON hash function, captures the hash function's permutation mechanism as its state transitions. Components of the hash function, such as input elements, S-boxes, and MDS matrices, are embedded in the state machine. Despite its secondary status, the POSEIDON SM interacts with both the Main SM and the Storage SM and is equipped with an executor and an internal set of verification rules in the PIL language.

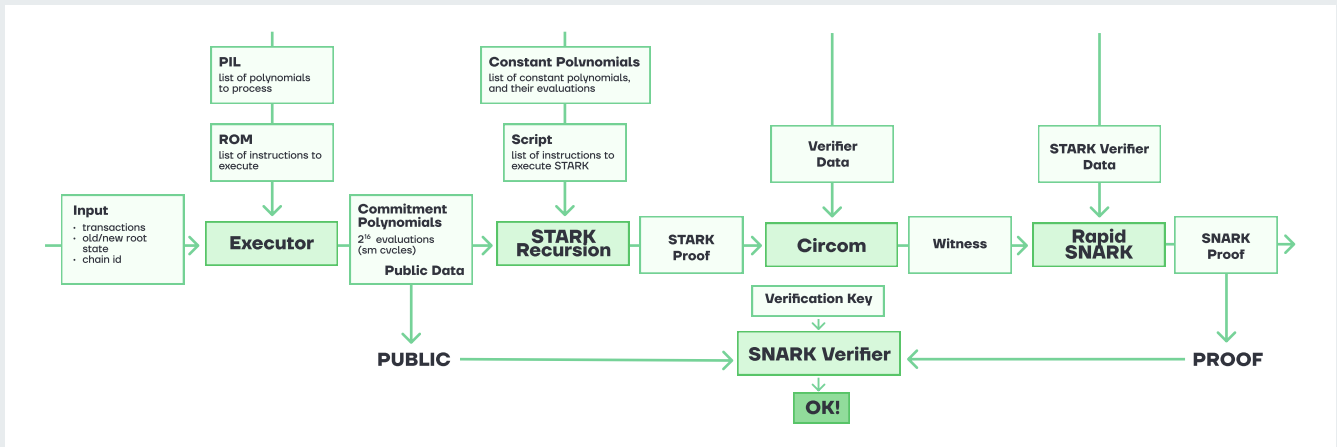


Figure 31. Components Of zkProver and their Interaction.

Source: Polygon Wiki: "zkEVM".

### • zkEVM Bridge

The zkEVM bridge, a smart contract, enables asset transfers between layers, denoted as LX and LY. The zkEVM L1-L2 bridge provides a decentralized interface for asset deposits and withdrawals. It comprises paired smart contracts, each deployed on a distinct chain. While the Bridge L1 Contract resides on the Ethereum Mainnet and orchestrates asset transfers across rollups, the Bridge L2 Contract, positioned on a specific rollup, oversees transfers between the Mainnet and the associated Rollup. This dual-contract system facilitates native asset migration across different L2 networks.

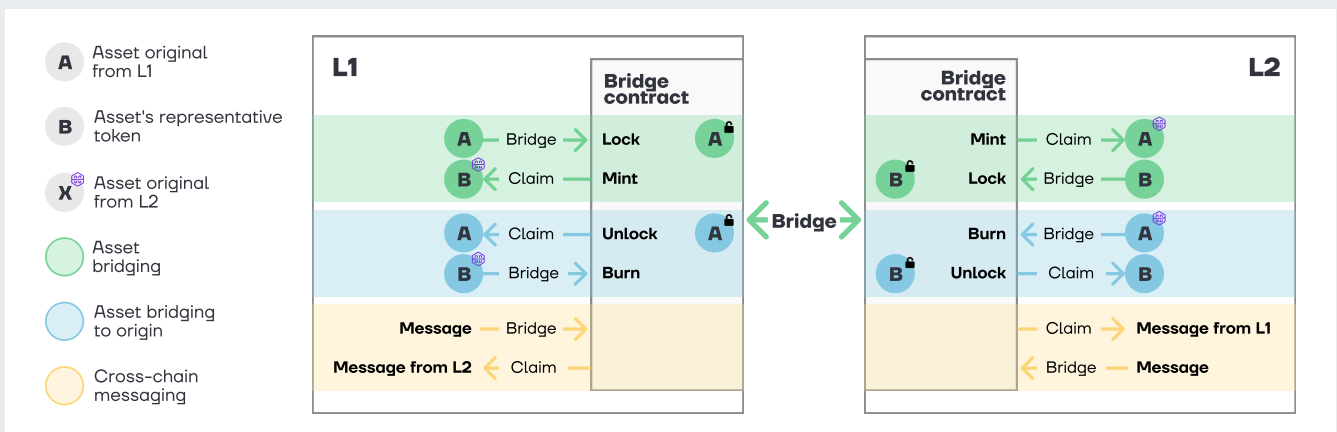


Figure 32. zkEVM Bridge Schema.

Source: Polygon Wiki: "zkEVM".

### • zkASM

The zero-knowledge Assembly (zkASM) defines the ROM of the processor in an abstract manner. This ROM instructs the Executor on processing different transaction types. Subsequently, the Executor produces a polynomial set representing the state transition, which the STARK generator then uses to create a proof verifying the accuracy of this transition.

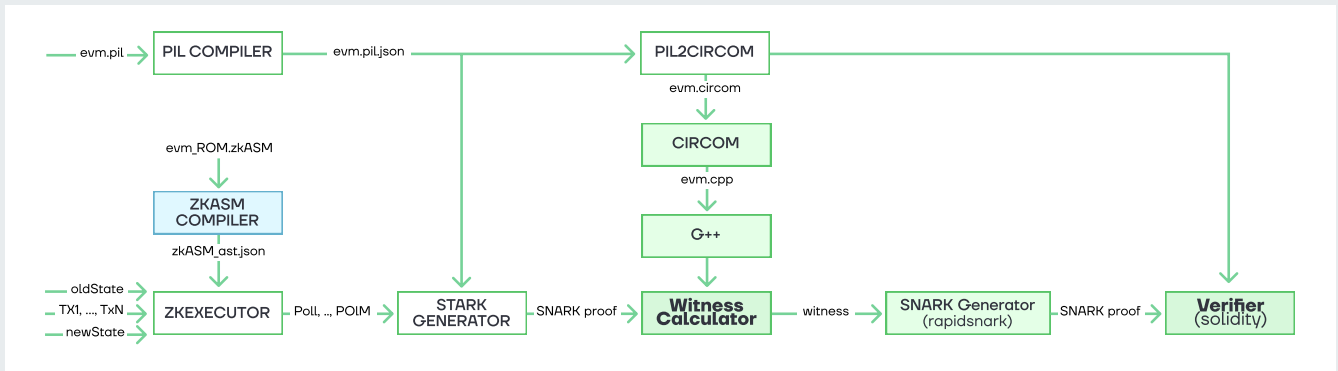


Figure 33. Executor update via zkASM.  
Source: Polygon Wiki: "zkEVM".

To find more about Polygon architecture, refer to the [ZK Rollups Landscape report](#) (page 43).

## EVM-Compatibility and Privacy

- Polygon zkEVM

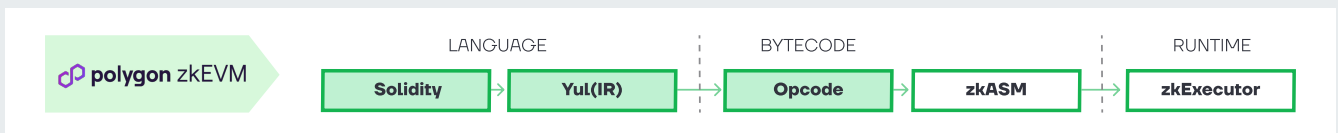


Figure 34. Polygon zkEVM.  
Source: zkValidator: "zkEVMs Beyond Polygon and zkSync".

Polygon zkEVM aims for EVM Equivalence, ensuring that applications, tools, and infrastructure native to Ethereum can be transitioned to Polygon zkEVM with minimal alterations. The benefits of this approach include:

1. Avoidance of code modifications that could introduce security risks.
2. Elimination of the need for further audits, conserving resources.
3. Maintenance of Ethereum's security and decentralization attributes since transactions finalize on Ethereum.
4. Utilization of the existing Ethereum developer community.
5. Facilitation of swift dApp integration due to inherent Ethereum compatibility.

The rationale for EVM Equivalence lies in Ethereum's extensive ecosystem of smart contracts, development tools, infrastructure, and its active community. Maintaining alignment with this ecosystem is crucial for scalability while providing a user experience reminiscent of Ethereum L1.

However, some differences exist in EVM opcodes on Polygon zkEVM: SELFDESTRUCT, EXTCODEHASH, DIFFICULTY, BLOCKHASH, and NUMBER. The zkEVM supports specific precompiled contracts like ecRecover and identity. Other precompiled contracts, when called, result in a revert, restoring all gas and indicating a failure. Notably, the current version of zkEVM does not support SHA256, BLAKE, and PAIRINGS precompiled contracts. Polygon zkEVM will achieve full EVM Equivalence once all pre-compiled contracts receive support.



• Polygon CDK

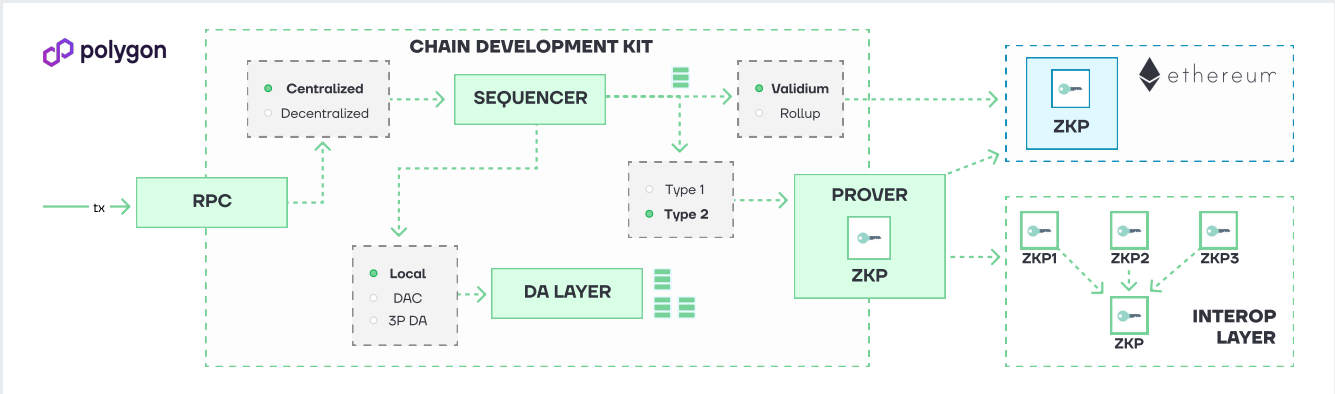


Figure 35. CDK High Level Architecture in connection with Ethereum and Interop Layer.

Source: Polygon: "Introducing Polygon Chain Development Kit (CDK)".

The Polygon CDK (Construction Development Kit) serves as an advanced, open-source framework tailored for crafting and implementing ZK-based Layer 2 blockchains on Ethereum. With its foundation deeply rooted in zero-knowledge proofs, it emphasizes transaction compression, scalability, and customizable features. Developers have the flexibility to design chains to their specifications, with choices ranging from rollup modes, ZK execution types such as zkEVM or MidenVM, diverse data availability methods, token customizations, Sequencer modes, and even configurable time frames for posting ZK proofs to Ethereum. Central to the CDK are three components: the Validium framework, the Data Availability Committee (DAC), and the LXLV Bridge. The Validium processes transactions off the Ethereum mainnet, ensuring data veracity with ZK-proofs. In parallel, the DAC, an assembly of nodes, secures consistent access to off-chain data, a vital function especially when Layer 2 operators might be inactive. The LXLV Bridge then bridges the gap, facilitating interactions and data migrations between varied blockchains within the CDK's ambit. An innovative feature is Polygon 2.0's Interoperability Layer, which aggregates ZK proofs from various Polygon chains and posts an integrated proof to Ethereum, effectively serving as a ZK-secured state coordinator and making cross-chain interactions seamless.

Every chain produced with Polygon's CDK is inherently interconnected with other Polygon chains, paving the way for seamless cross-chain transactions and shared liquidity. This design, coupled with Polygon's industry-leading ZK proof technology, like the efficient Plonky2 and the forthcoming Plonky3, ensures that chains deployed via the CDK leverage continuous developmental enhancements. The overarching vision of the Polygon CDK is not only to bolster processing efficiency and data integrity but also to revolutionize the Layer 2 blockchain transaction paradigm on Ethereum, creating an ecosystem where transactional ease meets technological sophistication.

## Ecosystem



Figure 36. Polygon Ecosystem.  
Source: Cryptomeria Capital.

## Roadmap



Figure 37. Polygon Roadmap.  
Source: Polygon Documentation.

- **October 2022** - Polygon zkEVM Testnet Launches.
- **January 2023** - Introducing Polygon Labs.
- **January 2023** - Polygon Foundation created.

### **Next notable developments:**

The engineering team at Polygon Labs published a proposal to upgrade Polygon PoS to a zkEVM validium, a first-of-its-kind decentralized L2 secured by zero-knowledge (ZK) proofs. This is a major milestone for the Polygon ecosystem, as it would enable Polygon PoS to become more secure and more performant while still being equally easy and affordable to use.

### **Also, this proposal includes:**

- PIP implementation and testing
- Upgrade I.E. PIP mainnet

## **Conclusion**

Polygon zkEVM is an Ethereum Layer 2 scaling solution that employs cryptographic zero-knowledge proofs to ensure off-chain transaction computation's validity and rapid finality. The primary objective is to handle state changes from Ethereum Layer 2 transactions and generate validity proofs through zero-knowledge techniques to authenticate these modifications. The core components of this system include the zkEVM Consensus Contract, zkNode, zkProver, and zkEVM Bridge. This system uniquely balances Ethereum's vast ecosystem's efficiency and security, striving for optimal performance and enhanced transaction speeds.

The zkEVM framework utilizes a Consensus Contract deployed on Layer 1 that integrates a new Proof of Efficiency approach, aiming for open participation in Layer 2 batch creation. This consensus model preserves unpermissioned batch production, prioritizes network performance, and ensures network security. A significant focus is placed on data availability; the system deliberates between a comprehensive ZK-Rollup or a Hybrid schema, the latter having configurations like Validium and Volition.

Polygon zkEVM is designed to be EVM Equivalent, ensuring that most Ethereum-native applications and tools can transition seamlessly to this platform. The overarching goal is to align with Ethereum's robust ecosystem, fostering scalability while retaining a user experience akin to Ethereum L1. Although the system currently exhibits some differences in EVM opcodes and lacks support for specific precompiled contracts, future iterations aim to achieve full EVM Equivalence, enhancing compatibility and utility for users and developers alike.

In June 2023, Polygon Labs proposed upgrading its flagship Polygon PoS sidechain to become a zkEVM Validium. This upgrade would result in the data availability for apps being handled by the validators, whereas the current zkEVM rollups have data availability directly on Ethereum.

Since September, the Polygon zkEVM has been live on Mainnet Beta, marking a significant milestone. The Dragon Fruit upgrade, also known as ForkID5, introduces support for the latest EVM opcode, notably making Polygon zkEVM the first Ethereum Layer 2 (L2) solution to support PUSH0. This development, achieved in collaboration with numerous clients of the Polygon CDK, sets the stage for substantial ecosystem growth in the coming year.

## Introduction

Taiko is dedicated to achieving Ethereum-equivalence (Type 1 ZK-EVM) while offering cost-effective bridge transactions, although it involves slower ZK-proof generation. Taiko's approach bears similarities to a hybrid between Optimistic Rollups and ZK Rollups. It introduces transactions with an initial level of trust but subsequently validates their integrity for enhanced reliability.

In terms of functionality, Taiko operates in a manner akin to Optimistic Rollups, allowing transactions to be permanently recorded on L1 even before ZKP generation and block validation. L2 nodes actively monitor the L1 state and arrange the transaction history on L2, relying on accurate hash values for verification.

The project is currently in testnet phase (Alpha-5). In this phase, proposers are required to acquire a bond from Provers to propose a block, which includes new rules for staking and slashing. Contributors can write smart contracts and launch nodes to test bridges and swaps on L2. The Mainnet launch is expected in the first quarter of 2024.

## Architecture and Fundamental Components

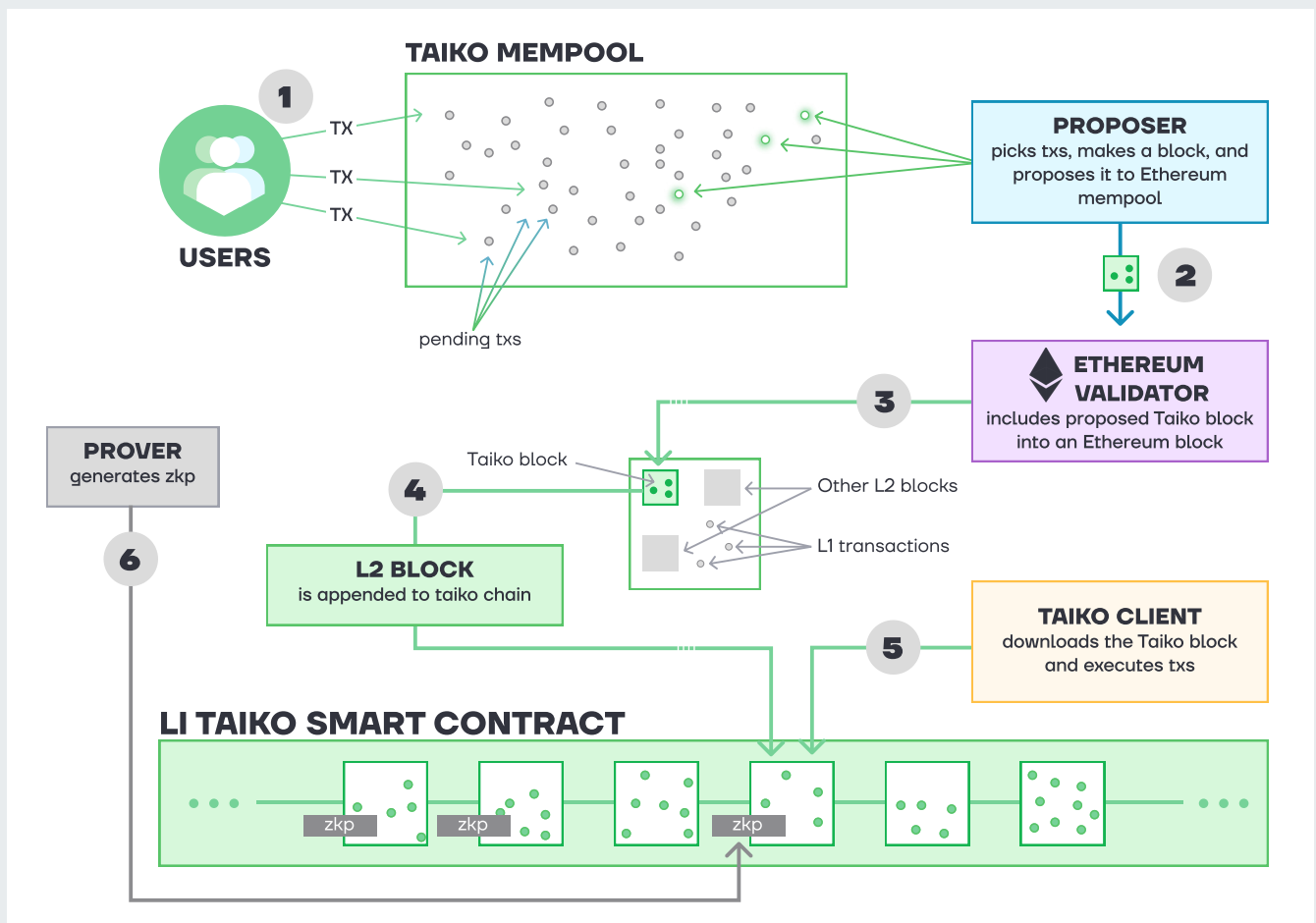


Figure 38. Taiko Protocol Design.

Source: Taiko Labs: "Taiko Protocol Overview".

## • Block proposals

Proposers track the Taiko network mempool for signed and sent transactions, collect them into a block, and submit it to L1 through the Taiko L1 smart contract. Ethereum validators determine the order of Taiko blocks on L1 independently, while Taiko L2 nodes monitor their state to understand which transactions have been added. There is no separate consensus on L2, but nodes synchronize and maintain a structured order of L2 transactions. Taiko blocks in Ethereum can be added even before generating the ZK-proof on L2. Once a block is added to the Taiko L1 smart contract, Provers attach the generated validity proofs to them.

- Blocks can be proposed and verified in parallel by different Proposers and Provers. Taiko supports up to 10,240 blocks without ZKP in a waiting mode on the L1 Execution Layer and reuses them to minimize the transaction cost.
- For aggregating and transmitting a block of transactions, Proposers receive an increased fee immediately on L2, part of which goes towards the fee for the L1 transaction, and the other part pays for the work of the Prover generating the ZK-proof for the block.

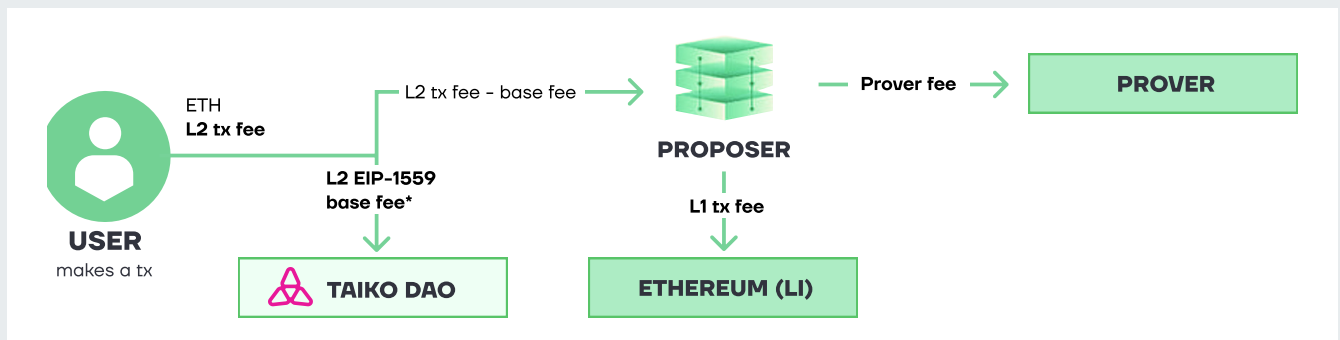


Figure 39. Block proposing.

Source: Taiko Labs: "Taiko Protocol Overview".

## • Block proving

When an L2 block is added to an L1 block, the L2 block is queued on the Taiko L1 smart contract, allowing nodes to detect it and track its validation status. For users, transactions are confirmed even before ZKP formation. Provers simultaneously fetch blocks from the Taiko L1 contract and verify transaction metadata, generating ZKPs for them. ZKPs will be generated if the given block and its "parent block" pass verification. Verified blocks have correct "before" and "after" hashes, enabling other smart contracts to monitor the L2 state. For most transactions, verification is irrelevant, mainly impacting intermediate transactions visible to all. However, L2→L1 transactions will require waiting for block ZKP validation to complete.

- At the time of the testnet launch, there was a centralized Oracle Prover responsible for regulating the reliability of generated ZKPs by verifying all transaction hashes and filtering out transactions with invalid proofs.
- The transaction fee on L2 Taiko consists of the base fee from L2 EIP-1559 (tips for Taiko DAO), the transaction fee on L1 (for Ethereum validators), the verification fee (provers fees), and the proposing fee (proposer fees).

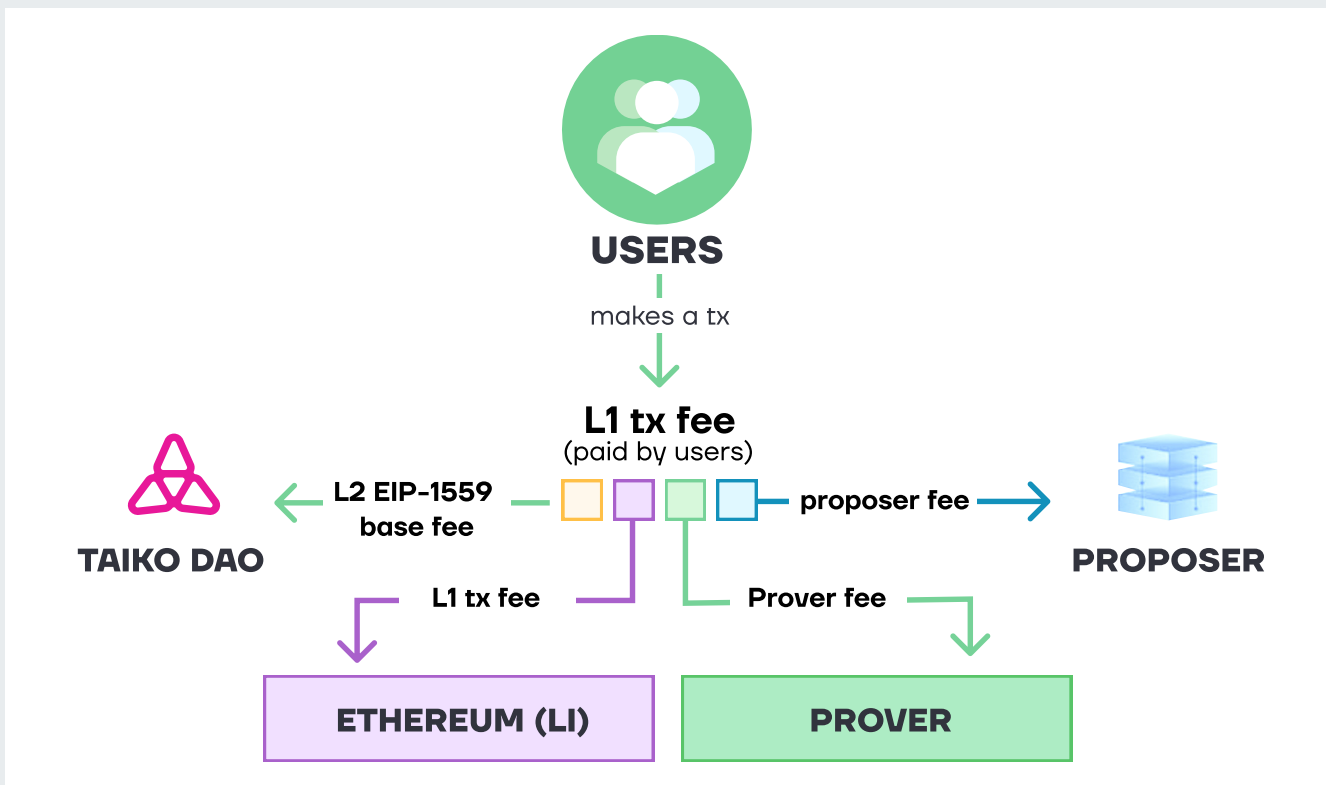


Figure 40. Fees distribution.  
Source: Taiko Documentation.

• **Inception Layers**

In July 2023, the team announced the possibility of launching L3 Taiko on top of L2, and within the Alpha-4 Eldfell test network, they introduced basic L3 layers. Similar hierarchy concepts have been promoted by Starknet, where in this case, L3 will utilize L2, just as L2 uses L1. However, given the architectural characteristics of Taiko, including an L3 block in the L1 mempool will be more challenging, so it makes more sense to use L3 for interactions on top of L2.

L2 for scalability, L3 for customizable features with less EVM compatibility:

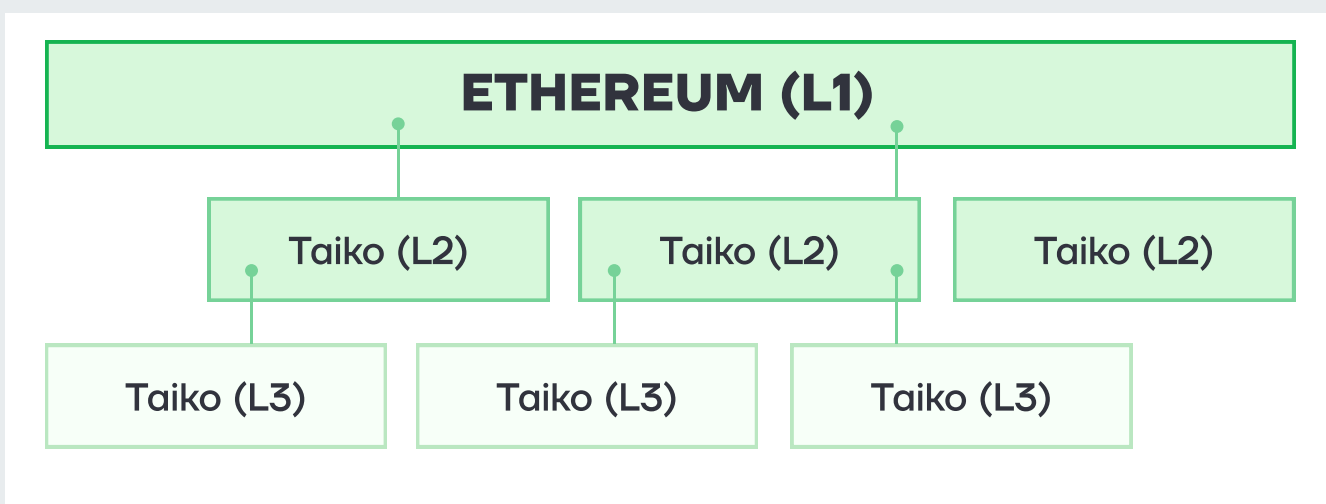


Figure 41. Inception Layers.  
Source: Taiko Documentation.

## EVM-Compatibility and Privacy

### • Taiko zkEVM

Taiko is a general-purpose zk rollup project aiming to support a Type-1 zkEVM, delivering developers a seamless experience. It achieved the Ethereum equivalent by using the same hash function, state structure precompiles, and consensus logic, earning it the label of zkEVM.

In the Taiko ecosystem, nodes take on the crucial role of aggregating and executing user transactions on Layer 2. They oversee the rollup chain's management and state evolution, with the Taiko protocol governing the rules and participants. Ethereum Layer 1 smart contracts serve as data availability mechanisms and ZKP verifiers.

Taiko is a fully permissionless and decentralized ZK-Rollup platform that is equivalent to Ethereum. This means that using Taiko is identical to using Ethereum. Taiko supports all EVM opcodes and provides the complete JSON-RPC execution client API, ensuring a seamless experience for users and developers. Furthermore, the Taiko client is constructed on top of Geth, ensuring compatibility with forthcoming Ethereum protocol enhancements.

It employs PLONKish ZK-SNARKs with a Halo2 proof system based on the KZG polynomial commitment scheme, which are considered neither transparent nor post-quantum secure.

## Ecosystem

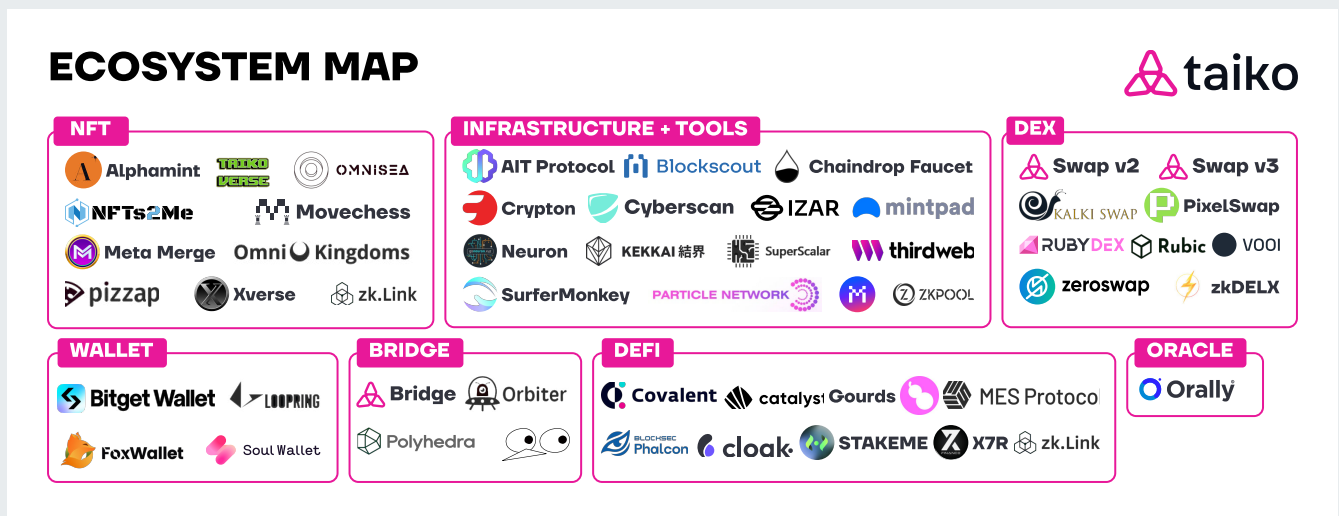


Figure 42. Taiko Ecosystem.

Source: Cryptomeria Capital.

# Roadmap

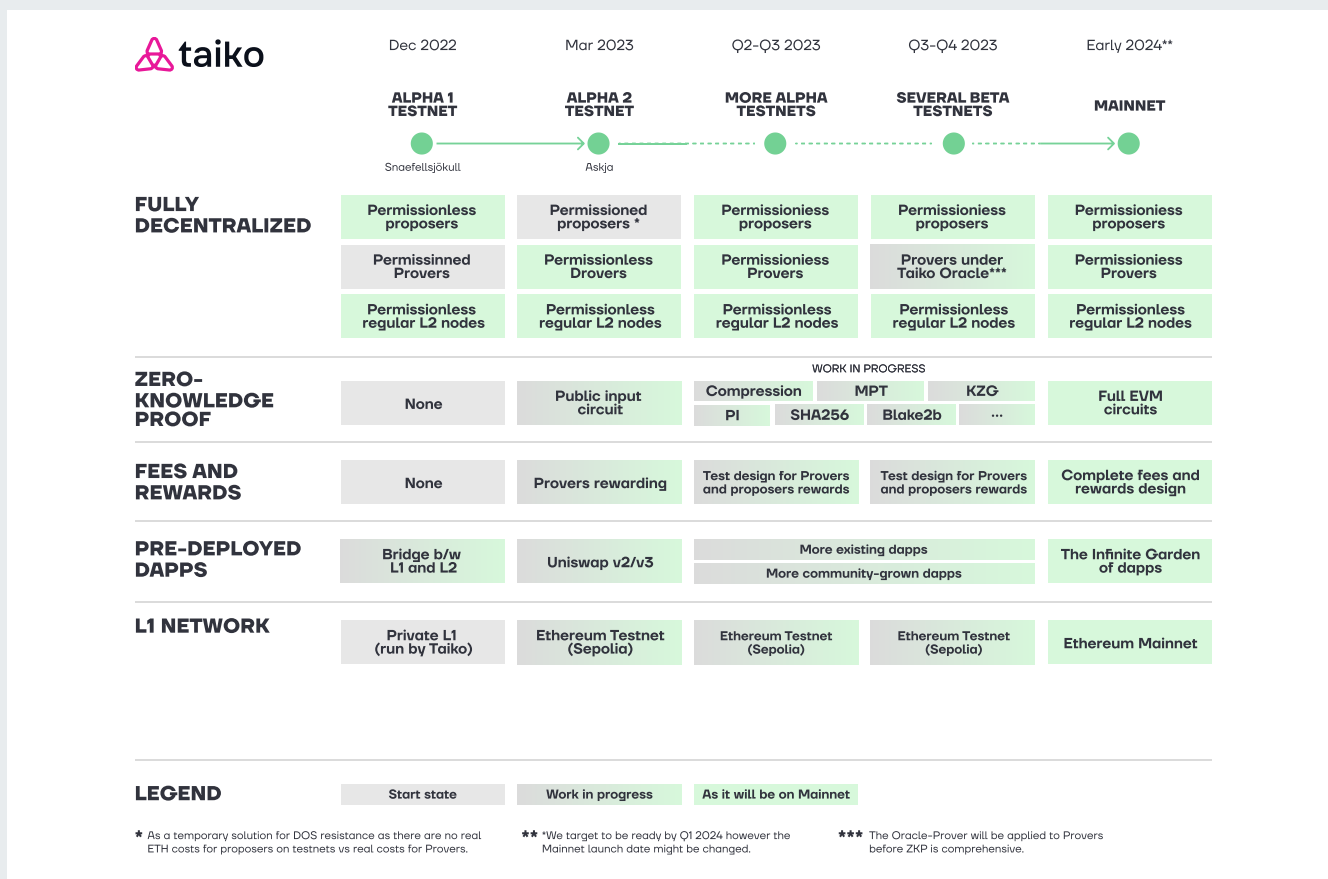


Figure 43. Taiko Roadmap.

Source: Taiko Labs: Taiko Roadmap.

- **Early 2022** - The first stage of the testnet was launched.
- **September 2023** - Alpha-5 testnet began.

### Next notable developments include:

- The full product launch is scheduled for early 2024.
- Taiko plans to launch with a decentralized system that includes proposers (Sequencers) responsible for submitting blocks and Provers responsible for generating ZKP).

## Conclusion

Taiko allows for the recording of transactions on L1 before the generation of ZKP and their subsequent block validation, a process that blends elements of trust and cryptographic verification. As of now, Taiko is in its testnet phase (Alpha-5) with a Mainnet launch projected for Q1 2024.

Central to Taiko's operation are two processes: block proposal and block proving. The former involves proposers collecting transactions into blocks and submitting them to L1, while the latter focuses on the generation of ZKPs after an L2 block's inclusion in an L1 block. This system allows for transaction confirmation even before the complete formation of ZKPs. The project utilizes a centralized Oracle Prover for ZKP reliability during its testnet phase and envisions a more inclusive pool of Provers in the future. Transactions fees on L2 Taiko are multifaceted, including fees for Ethereum validators, verification, and proposal among others.



Taiko is committed to developing a Type-1 zkEVM, aiming to provide a streamlined developer experience while maintaining alignment with Ethereum's structural elements. Nodes in the Taiko ecosystem play a pivotal role in executing user transactions on Layer 2 and overseeing its state progression. The potential introduction of an L3 on top of L2, known as the Inception Layers, offers an additional layer of scalability and customizable features.

Taiko is building the world's first Ethereum-equivalent (Type 1 ZK-EVM)  $e$ -based ZK rollup in order to scale Ethereum in a manner that emulates it as closely as possible — both technologically and ideologically. Effectively, Taiko offers the smooth UX of optimistic rollups with the added security of ZK proofs and much faster finality. Given Taiko is a Type 1 ZK-EVM, all existing Ethereum tooling will work out-of-the-box and any additional audits or code changes become redundant — meaning less overheads for developers.

“



**Brecht Devos**  
CTO and Co-founder



Taiko is a decentralized, Ethereum-equivalent ZK-Rollup.

Taiko's goal is to scale Ethereum without compromises. This goal directly guides us on many decisions. Taiko is Ethereum equivalent so that users and developers can keep interacting with the blockchain in a familiar environment. Taiko is a based rollup so that we can directly tap into the decentralization and features of Ethereum block builders and validators for building Taiko blocks. Taiko is a zkEVM so that we can scale Ethereum in a seamless and significant way without introducing additional trust requirements (except math). Taiko is a booster rollup so that we can seamlessly scale applications just by deploying more rollups. Taiko builds in the open, collaborating with the Ethereum Foundation and other projects.

At Taiko, we've always been very optimistic about the progress of zk, otherwise we wouldn't have set out to build an Ethereum equivalent ZK-EVM two years ago. Being optimistic about zk pays off, it allowed us to focus on making the best possible layer 2 we could from the start, not focusing on making temporary optimizations that impact the user and developer experience.

ZKPs are the only way to scale Ethereum in a way that has very few limits. A single party can verify work and prove it is correct while everyone else can just verify this proof. This not only provides scalability, it also provides a fast way to know something was done correctly. This process of creating a proof is already fast, but it is still limited by the computational complexity of the proof generation process. This not only affects cost, it also adds a delay. This cost and delay impacts where and when ZKPs can be used. However, this proof generation overhead (the overhead compared to just executing the work normally) has been going down rapidly and it's expected that this will continue. As it goes down, ZKPs will be even more useful, and it will be possible to use them for applications that are more cost and time-sensitive. Together with the rapid improvements in ZK tools that make it much easier to generate applications that can be proven, ZKPs will quickly break out of the few niche cases they are currently used in.

”

## Introduction

Linea is a developer-ready zkEVM rollup for scaling Ethereum dApps that is bootstrapped by Consensys via the full compatibility with the EVM that enables the direct deployment of already existing applications.

Linea architecture consists of three main elements: Sequencer, Prover, Bridge Relay. At the current state Linea has a Centralized Sequencer & Prover, which is rolled into one element and Bridge Relay.

## Fundamental Components

- **Canonical Message Service and Canonical Token Bridge**

The Linea **Canonical Message Service** is a system designed for seamless data transfer between the Linea and Ethereum, using mirrored smart contracts and an intermediary service, Postbots. They are 'actors' that 'listen' for calls being made to one of the contracts, either on Linea or Ethereum and pass the information submitted to the other network. Postbots will be decentralized in future to bridge data across the two networks.

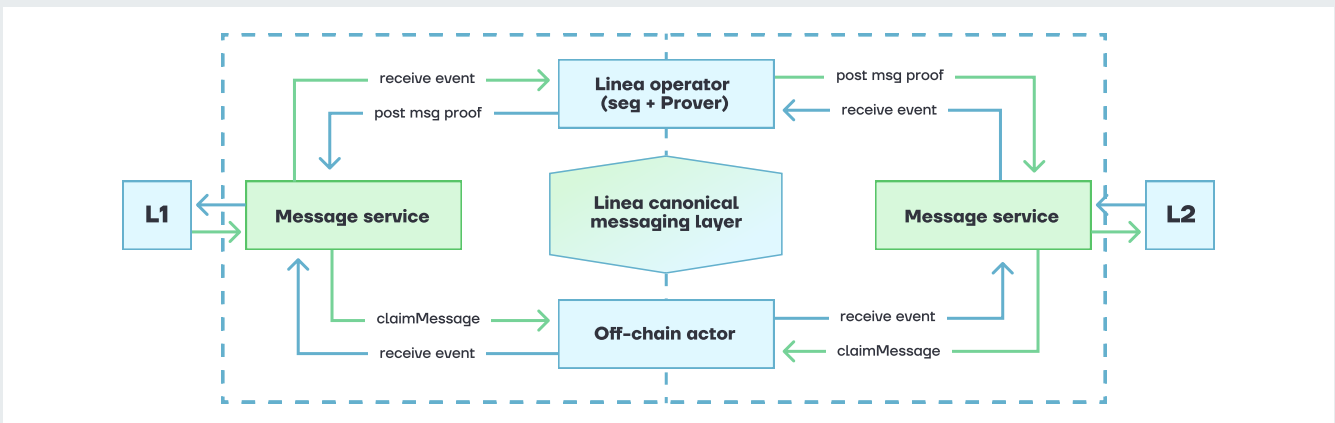


Figure 44. Canonical Message Service Overview.

Source: Linea Documentation.

**Canonical Token Bridge** is necessary to streamline liquidity and reduce complexities associated with multiple bridge systems. This bridge, introduced in the Alpha v0.2.0 upgrade, supports the transfer of ERC20 tokens between the Ethereum and Linea platforms using a standard lock-and-mint model and relies on the Canonical Message Service for information relay about deposits and withdrawals. The system allows for permissionless bridging, automatically generating a representation on Linea for first-time deposited tokens not already present on L2. Furthermore, an integrated token registry ensures the uniqueness of token addresses on Linea.

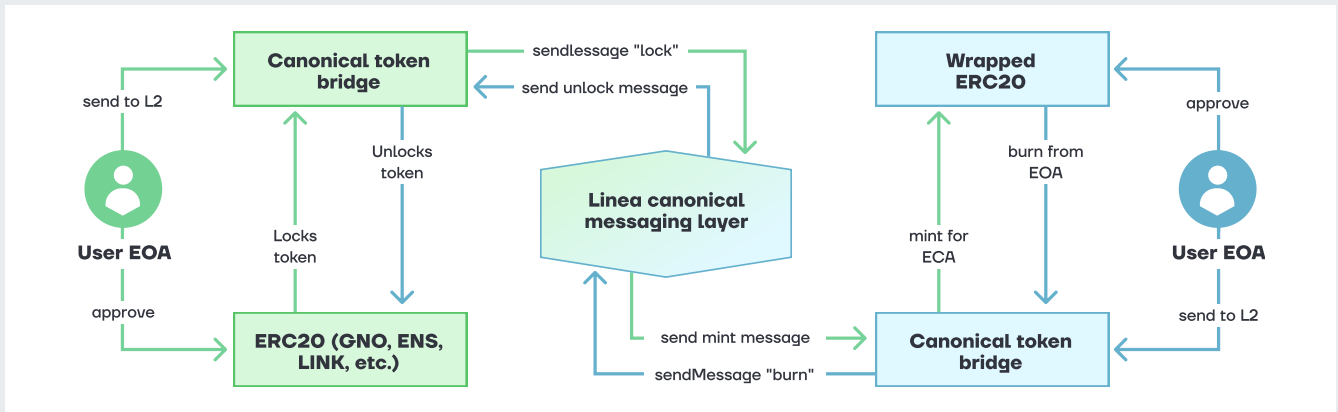


Figure 45. Canonical Token Bridge Overview.

Source: Linea Documentation.

At the heart of the Linea network is the coordinator, which manages the communication flow between Linea and Ethereum. The Sequencer, running on zkGeth, orders and processes transactions and prepares them for zero-knowledge proofs. After transactions are sequenced, they undergo conflation, a process that consolidates multiple block data. The EVM State Manager maintains the network's state, updating it using executed block data. This data is then used by the Corset, which expands the traces and prepares it for proof generation. Finally, the gnark system produces a zkSNARK proof, ensuring the transactions are validated and ready for submission to Ethereum.

For data availability, Linea employs numerous nodes, set up by Infura and managed by Consensys. These nodes handle both current transactional data and archive historical transaction data, offering transparent access akin to Ethereum while maintaining high network performance.

- **Coordinator**

**Coordinator** - Is a part of Linea that is responsible for overseeing various functions within Linea and ensuring the smooth flow of information between Linea and Ethereum. The Coordinator facilitates information transfer both internally among various segments of Linea's execution client and externally with other blockchains, Linea's data availability stack, and nodes synchronizing Linea's network state.

This component serves as Linea's consensus client. Its operations are characterized by a modular internal architecture where distinct systems and requirements operate in separate environments. Each of these modules interacts with the Coordinator by receiving inputs and providing outputs.

**linea-geth** - a version of geth that has been modified to work with zk-proving technology.

**Corset** is a component of Linea's architecture, functioning as "the Prover." It expands trace data for the generation of zero-knowledge proofs. When Linea's zk-EVM is updated, Corset creates a constraint system using mathematical rules.

This system is developed using a Domain-Specific Language in Lisp and is later converted to the Go programming language. For every block submitted to Linea, Corset ensures the trace data corresponds with gnark's application of the defined constraint system. This involves a process called "trace expansion," where data matrices are adjusted for compatibility with gnark, marking Corset's role in preparing data for proof generation in Linea.

**Hyperledger Besu** is an open source Ethereum client developed under the Apache 2.0 license and written in Java. It runs on public and private networks:

- Run Besu as an execution client on Ethereum

- Mainnet and Ethereum public testnets, such as Goerli and Sepolia
- Use private networks for enterprise applications requiring secure, high-performance transaction processing

**linea-besu** - In the next major release, the Sequencer will run the linea-besu client software, replacing the linea-geth client today. Linea-besu is a version of Besu that has been modified to work with zk-proving technology. As Linea progressively decentralized its architecture many different execution and consensus clients will be able to validate blocks on Linea, following the same client diversity philosophy seen on Ethereum mainnet.

- **Prover**

The proof system is mainly organized as a successive-compilation-step architecture. The “Arithmetization” is the set of constraints as expressed in the original posts. At a high level, the zkEVM arithmetization describes the EVM as a set of registers and their values over time (e.g columns). The columns constituting the zkEVM are bound to each other by constraints of various natures (inclusion, permutations, arithmetic constraints, etc).

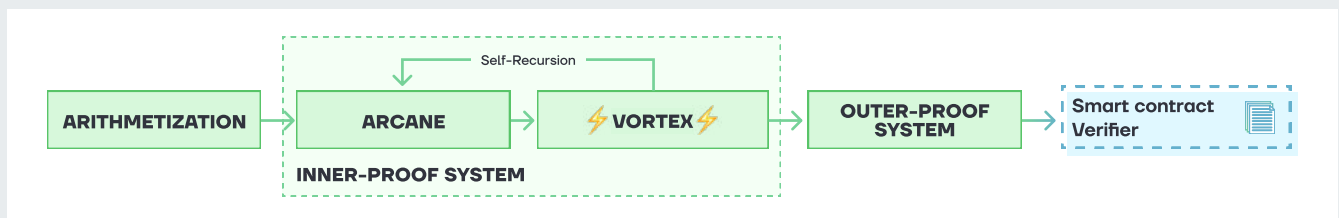


Figure 46. Linea zkEVM arithmetization.

Source: Linea Documentation.

Thereafter, the zkEVM arithmetization is compiled by Arcane, whose role is to convert the zkEVM arithmetization into a polynomial-IOP. It mainly leverages known techniques from Halo2, Plonk, Cairo, etc. From then on, Linea instantiates the polynomial-IOP into a concrete proof system using Vortex, a polynomial commitment scheme at the core of our proof system. Vortex is a plausibly post-quantum and transparent polynomial commitment scheme based on a lattice hash function. Although Vortex has  $O(n)$  proof size and verification time, it is equipped with a Self-Recursion mechanism which allows compressing the proof iteratively.

Once the proof is shrunk enough through self-recursion, Linea adds a final compression step using an outer-proof system (Plonk). This final compression step ensures that the proof is verifiable on Ethereum.

- **Gnark and PLONK Switch**

**Gnark** functions as the concluding segment of the Prover system. Outside of this context, gnark can also operate as an independent software, suitable for developing cryptographic Circuits for other projects. The gnark cryptographic library is one of the most used ZK libraries in the web3 industry: Algorand, Binance, Polyhedra, Celer, and many other projects are using and contributing to gnark. For Linea, gnark serves dual primary purposes.

First, it configures a series of "Circuits" or constraint systems, which are instrumental in generating a zk-SNARK proof verifiable within an L1 Ethereum environment. Secondly, gnark actively generates these proofs. To accomplish this, gnark's codebase is segregated into a frontend and a backend API. The frontend API facilitates the creation of cryptographic Circuits, effectively converting the Go constraint system from Corset into the desired constraints essential for SNARK proof formulation. The backend API, activated during runtime, leverages the previously established proving system to process

"expanded" trace data from Corset and generate the necessary proof. Once this proof, representing a set of authenticated and accurate transactions executed in an EVM environment, is crafted, it is then relayed back to its originating point, the Coordinator.

In Linea's Alpha v0.2.0 release, a shift from **Groth16** to **Plonk** was implemented for outer proofs. While Groth16 offers efficient proof generation and verification on Ethereum, it necessitates a new trusted setup ceremony for every modification to the arithmetic circuit. On the other hand, although Plonk requires slightly more resources for proof generation and yields larger proofs, it operates on a universal and updatable trusted setup. This change allows for the reuse of initial ceremony randomness for subsequent circuit updates, minimizing both operational efforts and potential risks associated with soundness guarantees.

- **4844, proof aggregation and data compression**

Linea will soon release a multitude of protocol upgrades which aim to significantly reduce gas prices. Firstly, Linea will be one of the first Layer 2 Rollups to use EIP-4844 to store calldata. This Ethereum upgrade reduces the costs of making data available on Ethereum for security and liveness guarantees.

Additionally, Linea will be implementing proof aggregation, whereby many batches of blocks and transactions are recursively proven into a single succinct SNARK proof that is verified on Layer 1. By increasing the number of transactions that can be finalized by a single proof, the fixed costs per batch will be amortized and lower L2 prices. Lastly, the Linea development team has announced it will be releasing a new data compression feature, such that the footprint of calldata published on Layer 1 is minimized to what is absolutely necessary, saving gas costs and thereby making transaction fees on Linea almost negligible.

- **Linea Stack**

Linea has announced that its software will be made open source in the next major release. This means the Linea Stack will be available for any ecosystem to create a new Layer 2 or a Layer 3 on top of Linea. Due to the industry-leading Prover technology (Vortex), the EVM-equivalence, and the client diversity (linea-gets, linea-besu, etc), this makes the Linea Stack an attractive addition to the growing appchain space. Moreover, as more enterprise and consortium chains consider migrating to use rollups anchored into Ethereum Mainnet, the familiar Besu client and EVM-compatibility provide a seamless transition for corporate entities to fully enter Web3 and the greater Ethereum ecosystem using Linea Stack software.

## **EVM-Compatibility and Privacy**

- **Linea zkEVM**

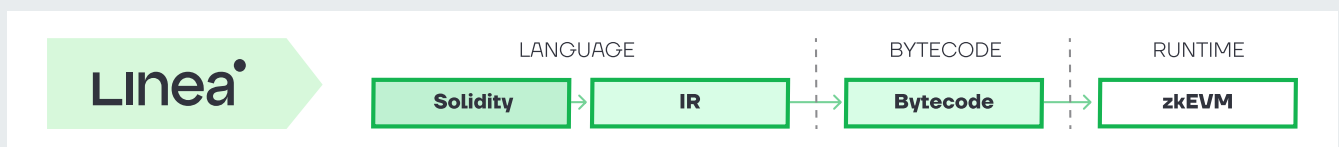


Figure 47. Linea zkEVM.

Source: Linea Documentation.

Linea is a Type 2 zkEVM, it runs an execution environment equivalent to Ethereum therefore Linea is not just EVM-compatible, it is EVM-equivalent. As it was stated earlier, at the core of Linea, the Sequencer operates on linea-gets, closely mirroring Ethereum's foundational operations.

The focus on processing trace data, expanded via Corset and culminating in zkSNARK proofs through gnark, further guarantees that transactions align with Ethereum's EVM standards. Moreover, Linea's support for the solc compiler and Ethereum JSON-RPC API standard underscore its seamless EVM-aligned design.

## Ecosystem

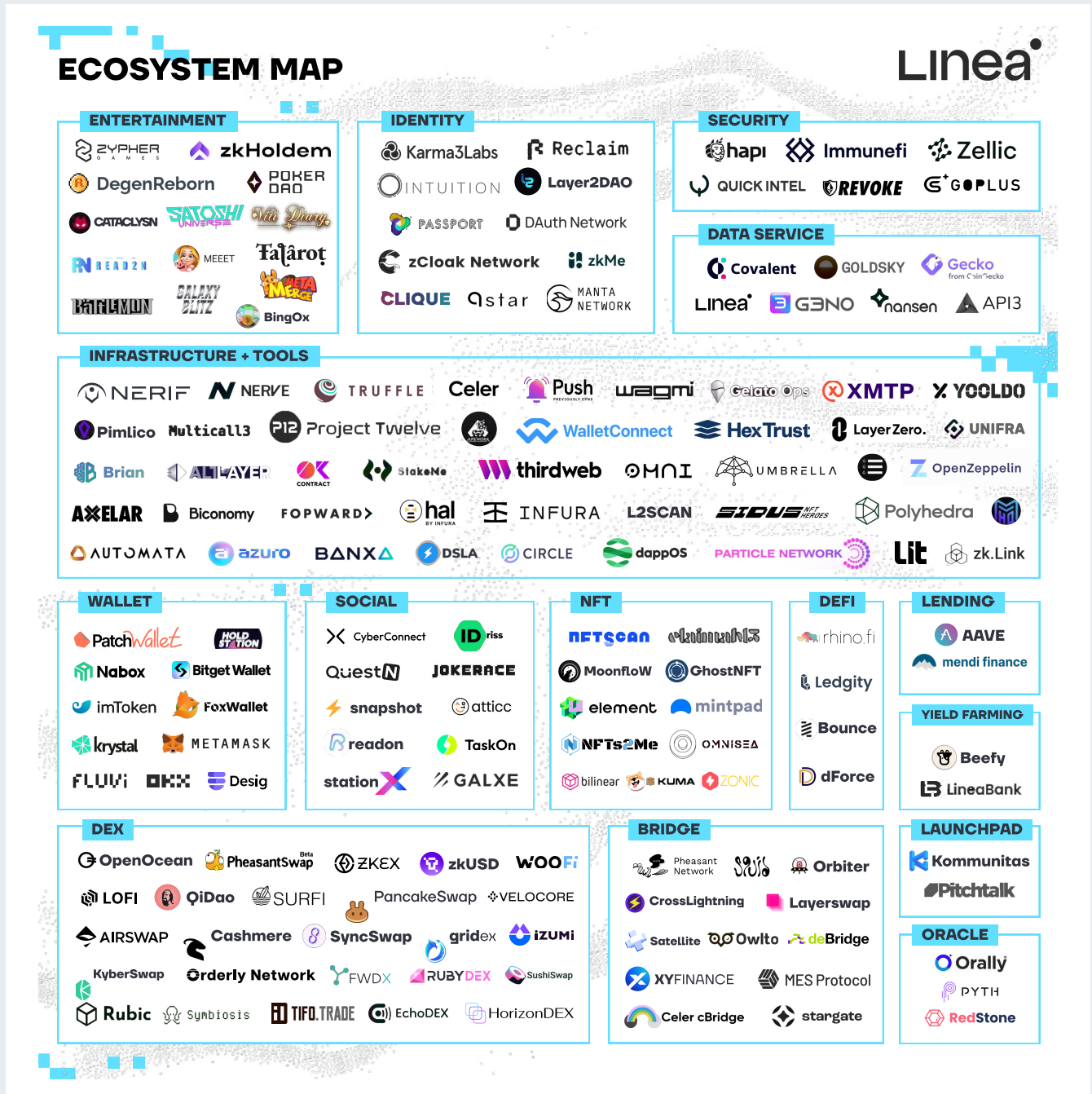


Figure 48. Linea Ecosystem.

Source: Linea Ecosystem and C98 Analytics.

## Roadmap

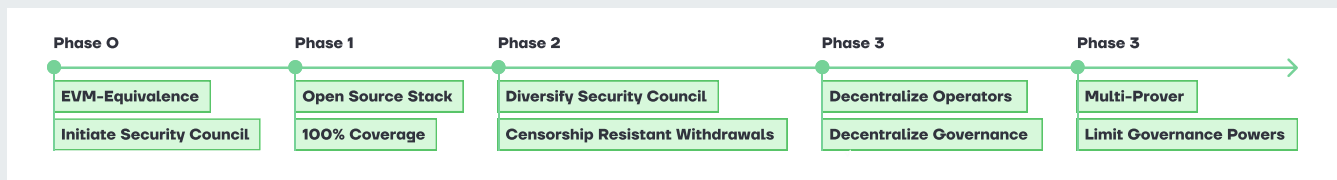


Figure 49. Linea Roadmap.

Source: Linea Documentation.

Linea has published a progressive decentralization and trust minimization roadmap. This includes decentralizing both operator roles (Sequencer, Prover) and governance. Notably, Phase 4 of the roadmap outlines Linea's plans to become a multi-Prover rollup. This architecture relies on multiple diverse implementations of a zkEVM Prover to generate a proof of a batch, providing even more guarantees around the validity of a state transition and mitigating the risk that there is a fault in the ZK circuit. This is especially important as the EVM spec continues to evolve and ZK teams are required to update, test, and audit their circuits. In fact, this is the same approach that Ethereum Mainnet has by using multiple client implementation (Geth, Besu, Nethermind, etc) such that a bug in one client does not bring down the whole network.

**Phase 0:** Linea's Mainnet Alpha is launched with its zkEVM, allowing for EVM-equivalent functionalities and portability. A Linea Security Council is established to monitor and secure the network, and client software is made public for network state verification.

- **Security Council** is an entity established during Linea's Mainnet Alpha launch. Its primary role is to monitor the Linea network, protect its users, and mitigate risks associated with the new production system. The Security Council operates through a multi-sig Safe contract, which means actions carried out by the council require a certain threshold of signatures. As Linea's network evolves, plans are also in place to diversify the council's membership to avoid concentration of power and to ensure balanced representation and decision-making.

**Phase 1:** Linea goes transparent by making its software stack open source under the AGPL-3.0 license and focuses on providing comprehensive EVM support through the zkEVM arithmetization, ensuring trustless execution for all EVM operations.

**Phase 2:** Linea's Security Council diversifies to prevent power concentration, with a strict multisig threshold maintained. A pivotal change ensures users can initiate exits from the rollup without potential interference, granting them unobstructed access to their assets.

**Phase 3:** Decentralization is at the forefront, with the roles of Provers and Sequencers opened up to the community. Governance is democratized, offering all stakeholders an opportunity to direct the course of Linea's future.

**Phase 4:** Resilience and trust mitigation are enhanced through a multi-prover system for the zkEVM. Governance powers are restrained, especially regarding rollup logic changes, ensuring a more immutable and decentralized approach.

## Conclusion

Linea, bootstrapped by Consensys, is an advanced zkEVM rollup solution designed to scale Ethereum decentralized applications (dApps). It aims to enhance the scalability and performance of Ethereum-based applications while ensuring full compatibility with the Ethereum blockchain. This allows for direct deployment of pre-existing applications without the need for significant modifications. Linea's

architecture comprises three main elements: Sequencer, Prover, and Bridge Relayer, with a current centralized model transitioning to a decentralized one in future phases.

At the heart of the Linea network is the Coordinator, a component that orchestrates communication between Linea and Ethereum. This system manages transaction ordering, processing, and the generation of zero-knowledge proofs, ensuring the validity and authenticity of each transaction. Key elements of this architecture include linea-`geth` (a modified version of the Ethereum client `Geth`) and the Corset and Gnark systems, which respectively prepare trace data and produce zkSNARK proofs for validation. These components work in harmony to maintain a processing flow that mirrors Ethereum's foundational operations.

One of Linea's standout features is its EVM-equivalency, providing an execution environment identical to Ethereum. This EVM-alignment ensures seamless interaction with Ethereum's standards.

“



**Declan Fox**  
Product Lead

# Linea

Linea is a developer-ready ZK rollup powered by [Consensys](#), enabling the next generation of Ethereum builders.

At Linea, our vision isn't just anchored in the promise of blockchain technology, but in the transformative power of scalability and community. Imagine a world where developers aren't limited by expensive gas fees and where transactions happen at the speed of thought. That's the world Linea is building towards with its state-of-the-art zkEVM. We're not just talking about small-scale improvements; we're pushing the boundaries with features like EIP-4844, advanced data compression, and proof aggregation. These aren't just buzzwords - they're tangible advancements that unlock a faster, cheaper, and more efficient decentralized ecosystem.

One of Linea's standout features is our commitment to diversity—not just in our passionate community, but in the technology that drives us. With a range of clients and our progress towards a multi-prover system, we ensure robustness and resilience in every step. And while we're proud of our tech, we understand that the future is collaborative. Our close partnerships with industry giants like MetaMask and Consensys don't just position us as key players; they underline our dedication to the long game in the blockchain world.

But here's the real magic: for developers, Linea feels like home. Our EVM-equivalence ensures that the onboarding process is seamless. Instead of grappling with new systems or codes, developers find a familiar environment, making the transition to Linea as intuitive as it gets. We're not just another blockchain solution; we're the bridge to the future of Web3, making the digital realm more accessible, efficient, and inclusive for everyone.

”



## Introduction

Loopring is an open-source, non-custodial exchange and payment protocol. It operates without requiring trust between participants due to its integration with zkRollup, ensuring assets remain under user control with security equivalent to Ethereum. The protocol enhances the scalability of decentralized exchanges and payments by processing numerous requests off-chain and validating their correctness using Zero-Knowledge Proofs (ZKPs), thereby circumventing Ethereum's performance limitations.

## Architecture and Fundamental Components

- **DeFi specification**

Loopring operates as a decentralized protocol leveraging zero-knowledge proofs to encode the process of order matching and settling. The translation of logical constructs to practical operation ensures the accuracy of order matching and adheres strictly to the price parameters set by users. Such a setup is insulated from third-party interference, reinforcing process integrity. An analogy can be drawn wherein a user's intent to interact with a Layer 2 DeFi product is likened to placing an order. Upon the presence of a counterparty, instant L2 DeFi Port interactions are feasible.

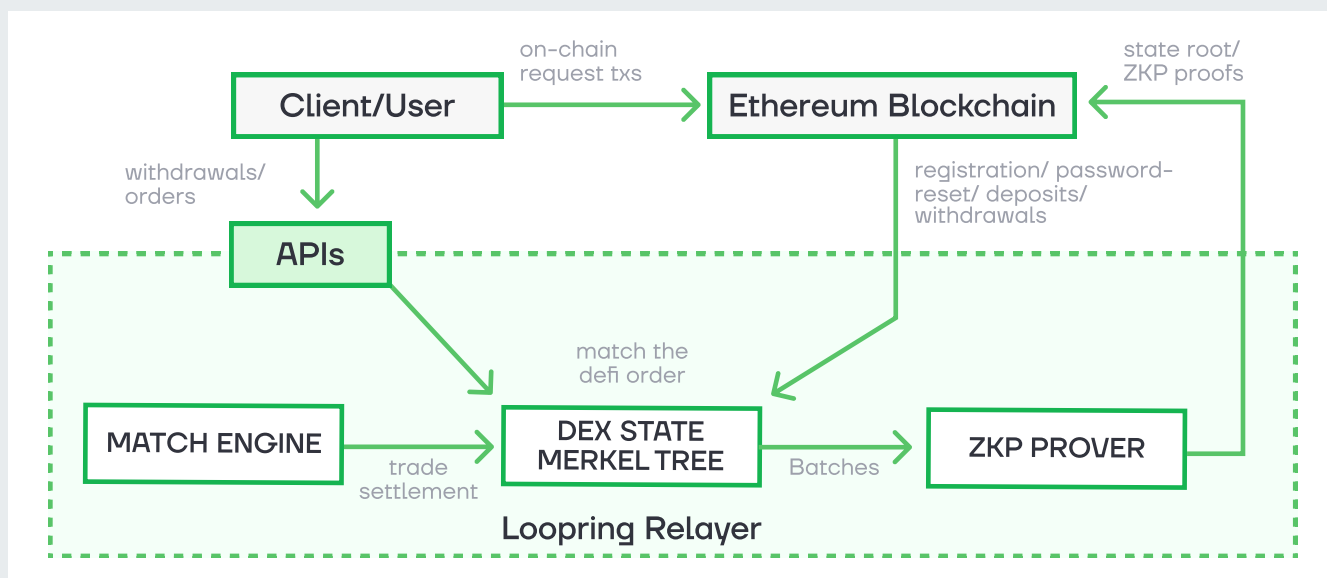


Figure 50. Overall Architecture of Loopring.

Source: Loopring Documentation.

In collaboration with Lido on Ethereum Layer 1, Loopring taps into its liquidity reserves. This involves the conversion of wstETH followed by its deposit onto Loopring L2. Upon staking ETH on L2 using Loopring's DeFi products, the system's matching engine pairs a wstETH sell order. After the validation stage via the matching settlement circuit, a trade-off between ETH and wstETH ensues. The reverse process is implemented for staking withdrawals, wherein Loopring provides a counterparty buy order based on the L1 price of wstETH, enabling conversion from wstETH back to ETH. The crux of this operation is its decentralized and non-custodial nature.

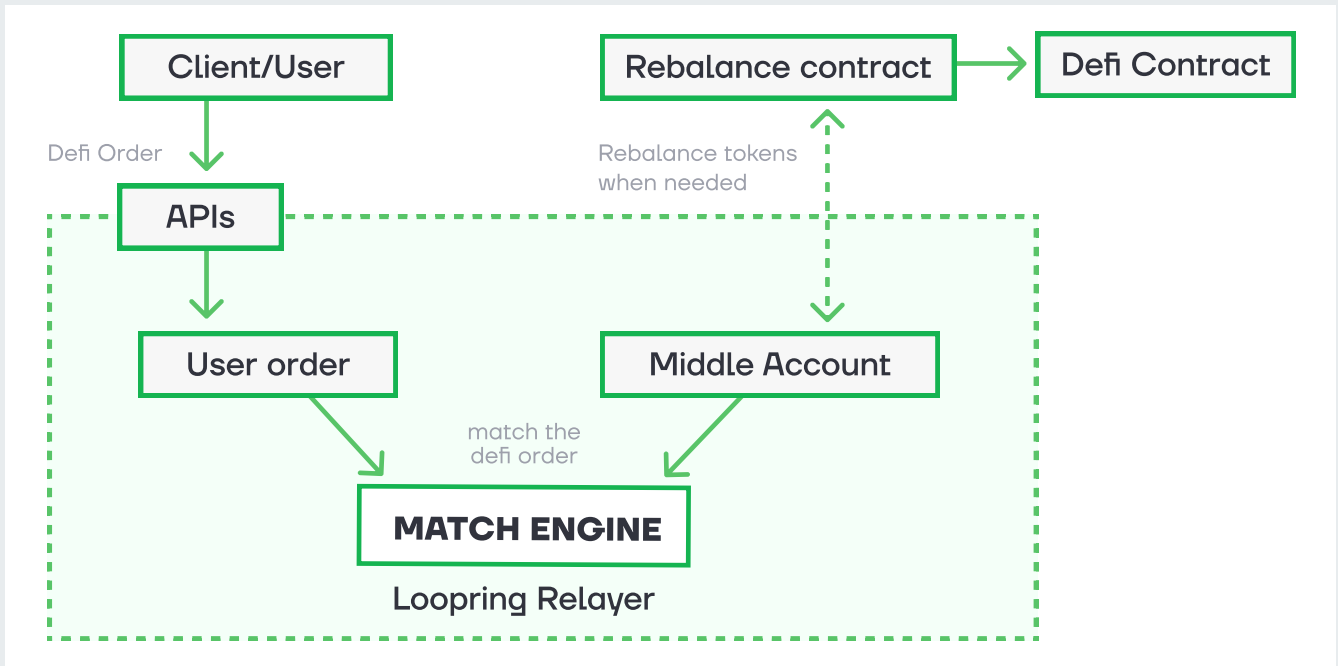


Figure 51. Looping Relayer Overview and Interaction with Rebalancing Contract.  
Source: Looping L2 DeFi Port.

Looping's liquidity management parallels the functionality of an intermediary financial institution, accommodating user deposits and withdrawals. Minor discrepancies in these amounts bypass the need for L1 interactions. However, larger imbalances or marked wstETH value appreciation necessitates a rebalancing shift to L2. This entails a series of steps involving asset withdrawal to L1, interaction with other DeFi protocols, and a subsequent redeposit to L2, all orchestrated by automated smart contracts.

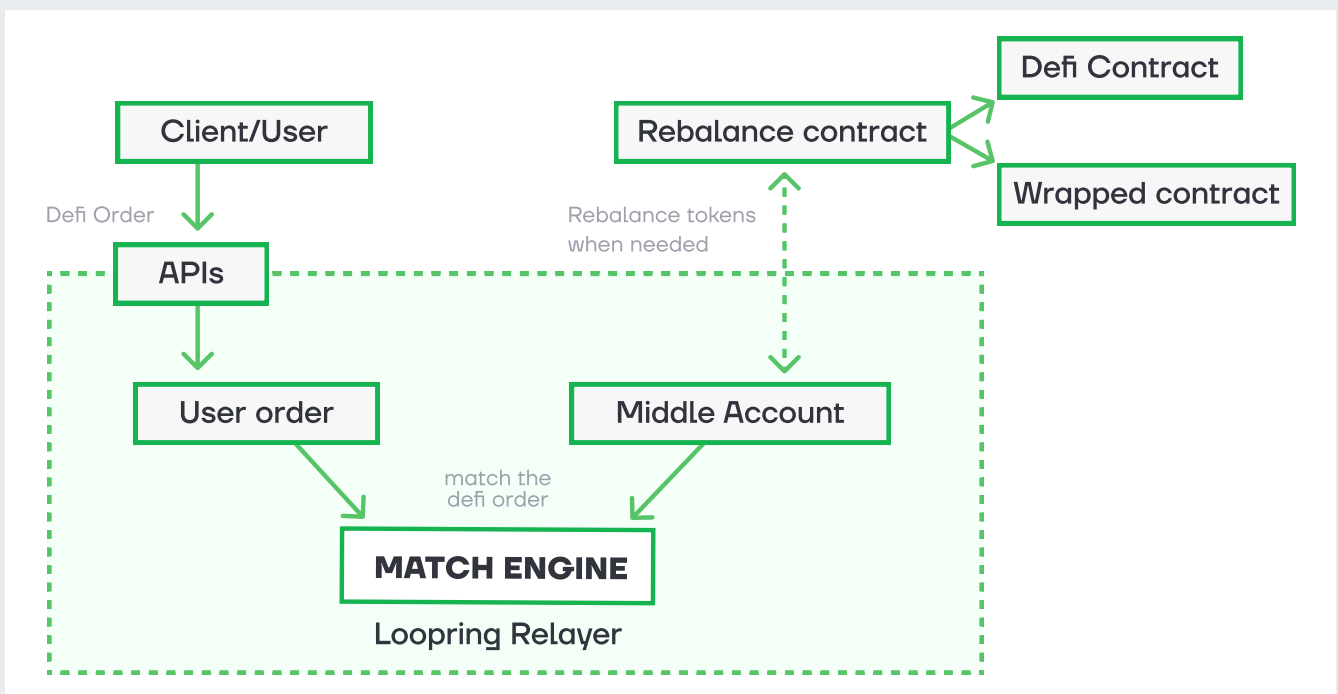


Figure 52. Looping Relayer Interaction for wstETH.  
Source: Looping L2 DeFi Port.

The architecture also factors in scenarios of fund insufficiencies. Here, an approach reminiscent of traditional banking is employed, utilizing a robust API known as "asset locking". Primarily employed within Loopring's order book, this API locks assets temporarily, pending the identification of a matching counterparty order. Furthermore, the design of Loopring's L2 DeFi access mechanism embodies the principle of user asset control, ensuring user autonomy over asset redemption and interaction.

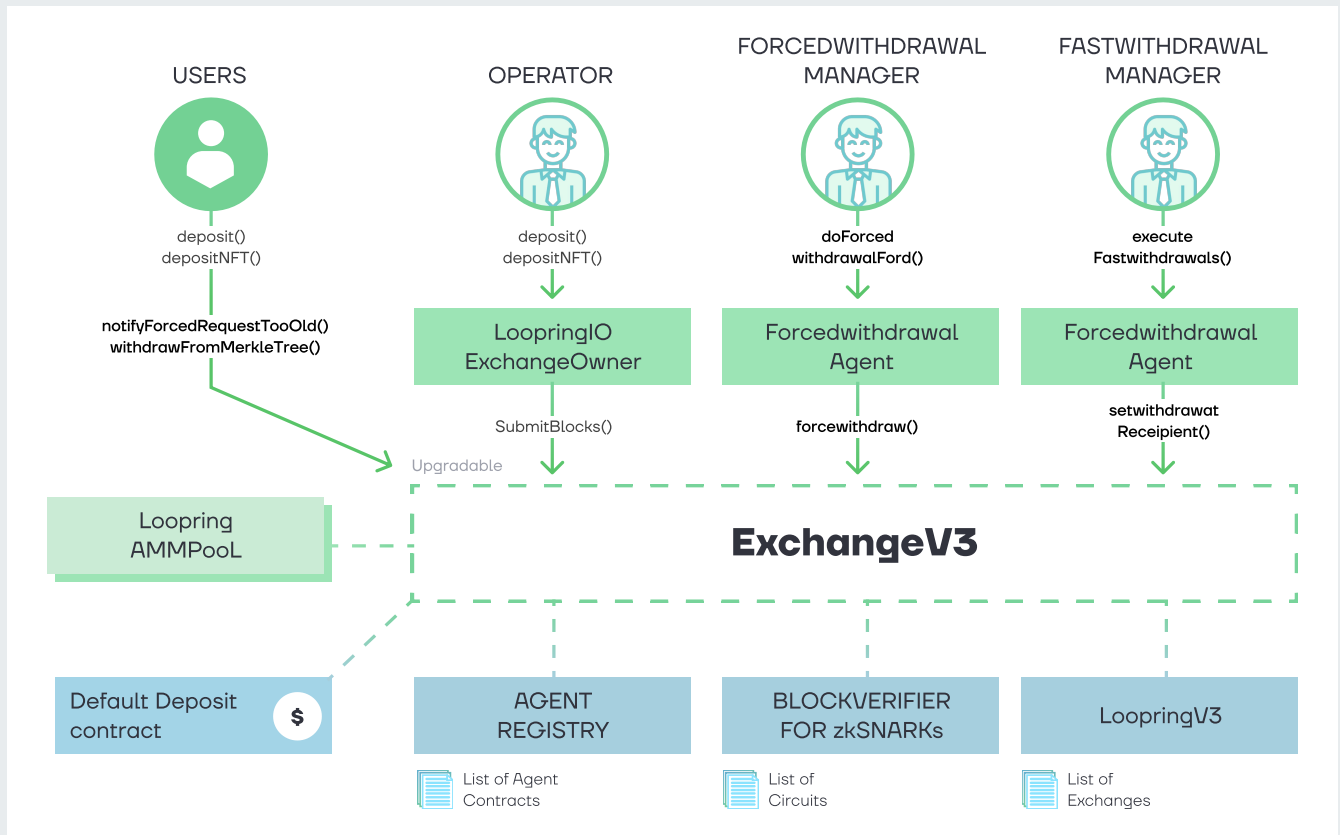


Figure 53. The system of Loopring's smart contracts.  
Source: L2Beat.

#### • NFT services

Also, it will be valuable to mention Loopring zkRollup now supports NFT minting, trading, and transfers, directly on L2.

- Any NFT minted on L2 can be withdrawn to L1.
- Both ERC1155 and ERC721 NFT token standards are supported.
- L1 NFTs can be deposited to L2.
- No restrictions: all L2 accounts can mint NFTs.

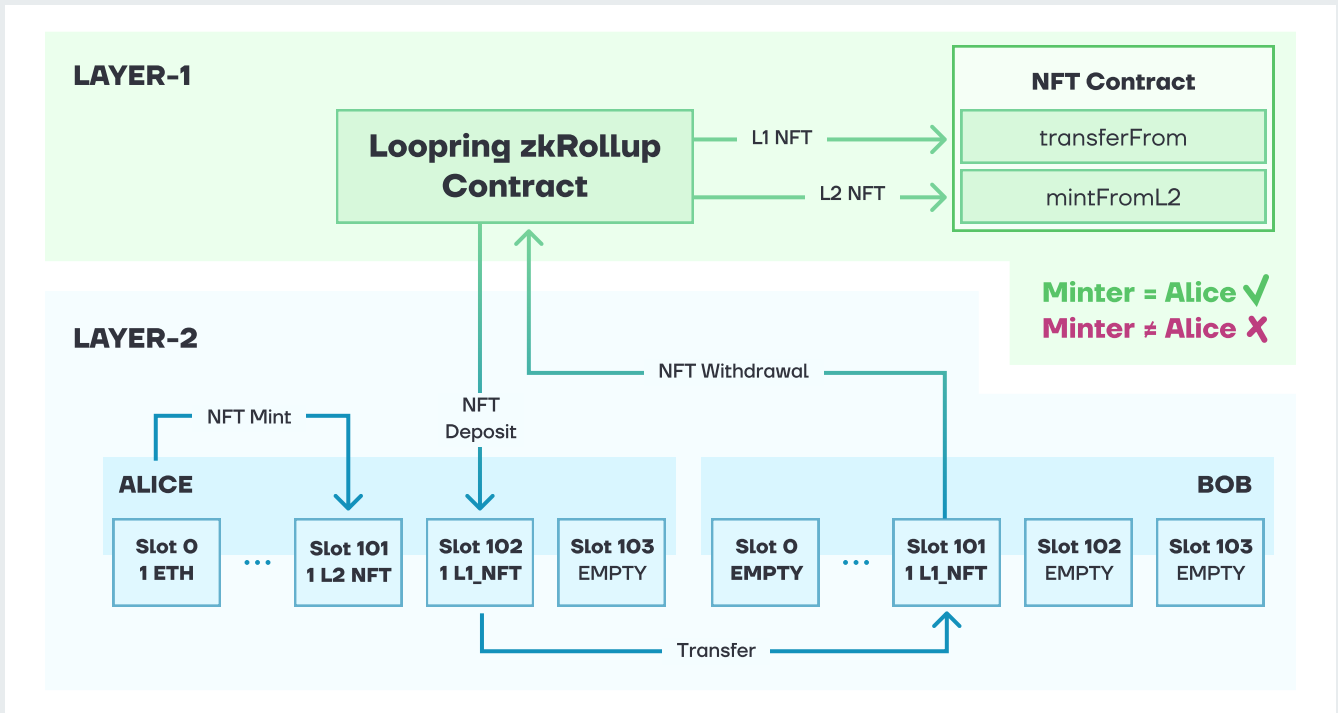


Figure 54. NFTs on Loopring.  
Source: What is Loopring?

- **Loopring Layer 3**

Loopring L3 (testnet version), launched in Q3, remains accessible for testing on the Taiko L2 alpha testnet. The initiative involves the migration of the generalizable smart contract layer to L2 and the migration of an increased user base and applications to L3. This strategic move is expected to significantly reduce user costs to a few cents and enhance the overall user experience.

## EVM-Compatibility and Privacy

- **Taiko zkEVM**

Loopring supports scalable trading and transfers rather than arbitrary EVM actions. With the introduction of Loopring L3 and the implementation of Taiko zkEVM, this shift promises a more cost-effective and faster protocol. These improvements are likely to incentivize more users to remain within the Loopring ecosystem. Furthermore, this internal growth extends to encompass existing DEXs, dApps, and L3 compatibility with the Taiko zkEVM, collectively contributing to enhanced performance and the attraction of a wider user base.

- **Loopring zkSNARKS**

Loopring harnesses the power of zkSNARKs to ensure efficient and scalable transaction aggregation on its platform. Specifically, it aggregates multiple operations, such as transfers or trades, into a single proof that is subsequently processed on Ethereum. This aggregation considerably mitigates the gas overhead traditionally associated with individual on-chain operations.

In its cryptographic foundation, Loopring employs the BN\_256 elliptic curve, more commonly recognized within cryptographic circles as BN128. This particular elliptic curve is noteworthy due to Ethereum's native support for it via precompiled contracts. Ethereum's integrated support for BN\_256 facilitates a more gas-efficient on-chain verification of SNARK proofs. This synergy between Ethereum's

infrastructure and Loopring's chosen elliptic curve is pivotal in optimizing transaction throughput and cost-effectiveness.

Loopring ensures data availability by posting a compressed version of the account state on-chain. Even though this data is concise, it ensures that the full state can be reconstructed if necessary. The zkSNARK proof, once generated and submitted, is verified by the Ethereum Mainnet. After this on-chain verification, the bundled transactions are considered as finalized on Ethereum L1.

## Conclusion

Loopring is a non-custodial exchange and payment protocol on Ethereum, utilizing zkRollup technology to aggregate multiple transactions. It incorporates zero-knowledge proofs to process transactions off-chain while adhering to Ethereum's security protocols. This mechanism optimizes the number of transactions and reduces associated costs. Loopring has integrated with Lido on Ethereum Layer 1 for liquidity purposes and supports functionalities for NFT activities on Layer 2, accommodating both ERC1155 and ERC721 NFT token standards. Users can engage in NFT-related operations between Ethereum Layer 1 (L1) and Layer 2 (L2).

From an architectural perspective, Loopring aligns with Ethereum's existing structure. It employs zk-SNARKs to combine several operations into one proof, which is subsequently processed on Ethereum. This reduces the computational gas required for transaction verification. Loopring uses the BN\_256 elliptic curve (also known as BN128), which is supported by Ethereum, for efficient on-chain SNARK proof verification. To ensure data availability, Loopring stores a succinct version of the account state on the Ethereum blockchain. If needed, this compressed data can be expanded to its full state. Following on-chain validation, transactions are recognized as complete on Ethereum L1.

Loopring's deployment of L3 in Q3 and its ongoing availability for testing on Taiko L2's alpha testnet represent a crucial step in their roadmap. This strategic move demonstrates Loopring's commitment to advancing the efficiency and accessibility of their solution.

Within its ecosystem, Loopring's decentralized exchange operates using zkRollup to achieve scalability. The protocol also includes the Loopring Smart Wallet for mobile Ethereum transactions, which takes advantage of zkRollups for transaction speed and cost. The Loopring SDK is available for developers, allowing for protocol integration into third-party applications. Governance decisions related to the protocol are made through the Loopring DAO, enabling changes based on collective consensus. Furthermore, Loopring has incorporated NFT functionalities into several gaming apps and metaverse.

## Introduction

Kroma aspires to be a cutting-edge ZK Rollup, combining the strengths of optimistic and ZK rollups: high EVM compatibility, low fees, high throughput, and fast finality. Currently, it is an Optimistic Rollup with ZK fault proofs and a zkEVM from Scroll. Their goal is to shift to a ZK Rollup when ZK proof generation is more efficient.

## Architecture and Fundamental Components

Kroma is an EVM equivalent Zero-Knowledge Rollup (ZKR) that scales Ethereum. Specifically, in the testnet phase of Kroma, it can be characterized as an Optimistic Rollup (ORU) with ZK Fault Proof and a centralized sequencer and permissionless validator network with more than 30 active validators in the mainnet.

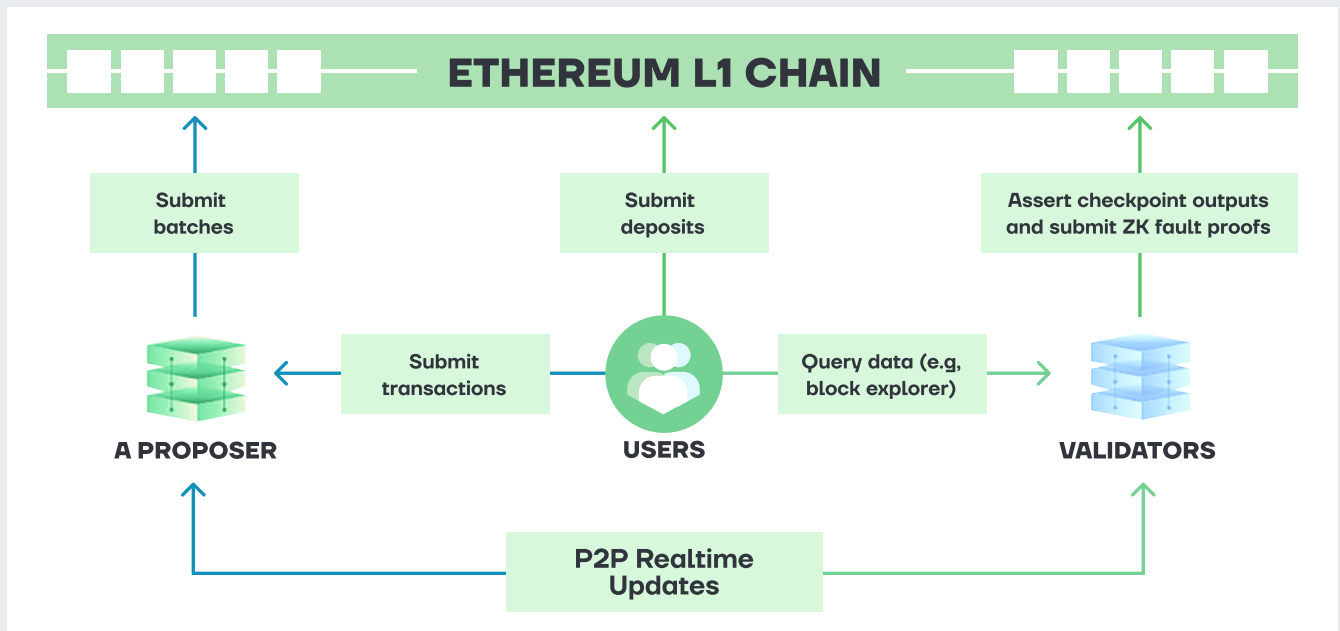


Figure 55. Who participates in Kroma?

Source: *An Overview of Kroma's Architecture*.

In Kroma's structure, there are three main roles: User, Sequencer, and Validator.

- **Users** can make deposits or withdrawals through a contract or send transactions to a Sequencer, much like typical transactions.
- **Sequencer** collect these transactions and organize them into blocks. These blocks then get transferred to the main layer.
- **Validators** check the blocks from the Sequencer. If they spot errors, they flag them and provide evidence of the error.

## Block Creation

- L1 and L2:** L2 creations reference L1, ensuring that user transactions on L1 can be incorporated into L2 creations. L2 structures created but not yet transferred to L1 are termed 'unsafe', whereas those fully derived from L1 are termed 'safe'.
- Integration Process:** To integrate L2 creations into L1, they are first compressed to save space. Given size limitations, these compressed sets can be further segmented before they are added to L1.

## Roles & Functions

- Sequencer:** Comprises a unit to add L2 creations to L1, a processing engine, and a batch handler. The engine is responsible for assembling blocks and managing states, while the batch handler manages the compressed L2 sets and their segments.
- Validator:** This role involves reading compressed L2 sets from L1 and constructing L2 blocks from them. It's similar to the sequencer but has a different component for validation.

## User Transactions

- Deposits & L2 Direct Transactions:** Users initiate deposit transactions on L1. Sequencer monitors these and incorporates them into L2 blocks. Users can also send transactions directly to L2.
- Withdrawals:** The validator checks the current status of the L2 chain and updates L1 at regular intervals, which helps in confirming transfers from L2 to L1.

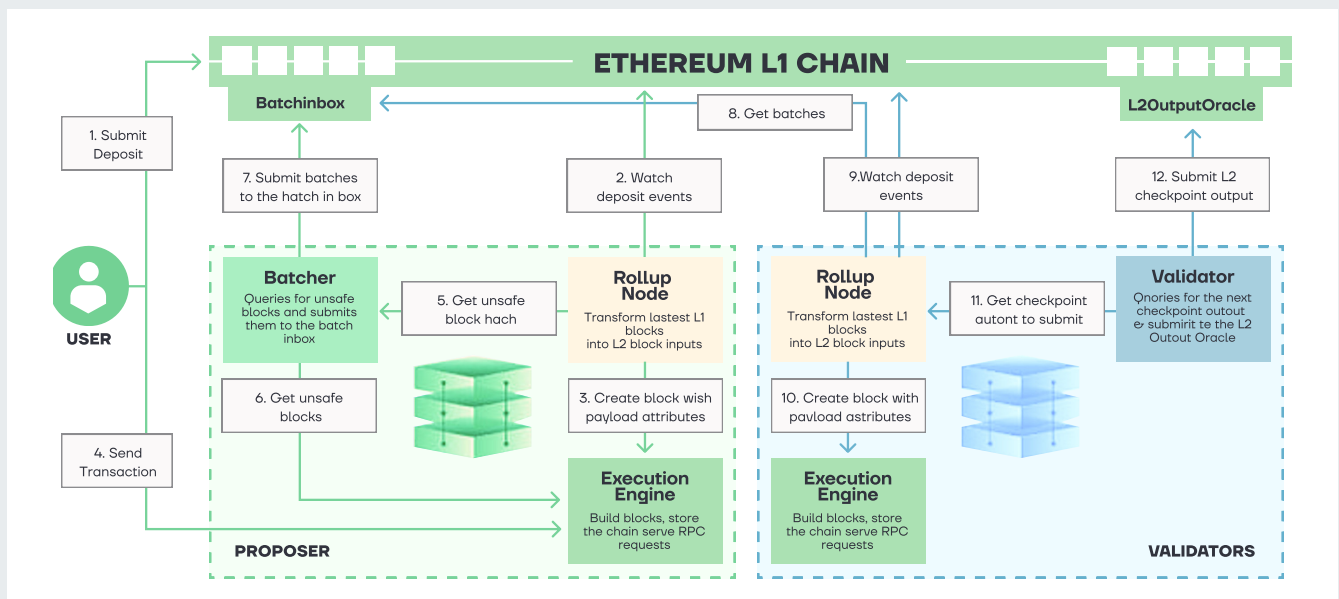


Figure 56. Deposits and L2 transactions.

Source: An Overview of Kroma's Architecture.

## User Withdrawal Process

- User initiates L2 to L1 transfer; Sequencer integrates latest L1 into BatchInbox.
- Validator submits a so-called output root and the output roots are finalized after 7 days if they are not challenged; user requests KromaPortal for withdrawal proof.
- After the output root is finalized, the user sends another transaction for withdrawal, assets are returned to the user.

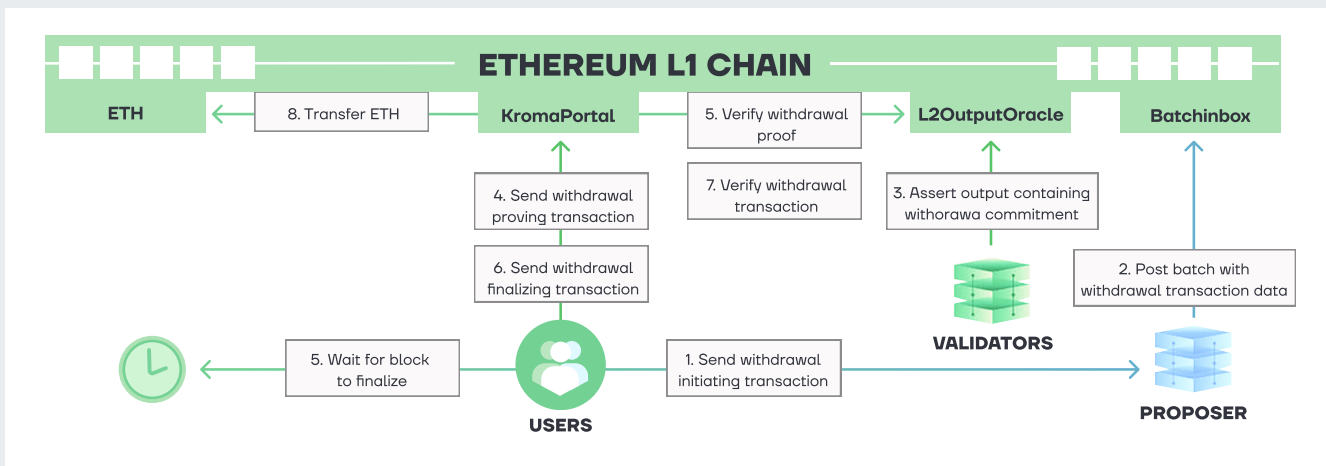


Figure 57. Withdrawals.

Source: An Overview of Kroma's Architecture.

## EVM-Compatibility and Privacy

### • Kroma zkEVM

Kroma in its final state is an EVM equivalent Zero-Knowledge Rollup, while as for now it can be characterized as an OR with ZK Fault Proof and a centralized Sequencer and permissionless validator network. ZK Fault Proof refers to the implementation of fault proof using zkEVM.

The Kroma Mainnet was launched on 6th September. Kroma implemented permissionless validator network and implemented zk fault proof using Scroll's zkEVM. Also they have constructed the Kroma Security Council, which currently has 8 members and 2 more members will join soon. Within this framework, validators have the authority to challenge what they deem to be an incorrect assertion presented by another validator. The individual taking on this challenging role is termed the 'challenger'.

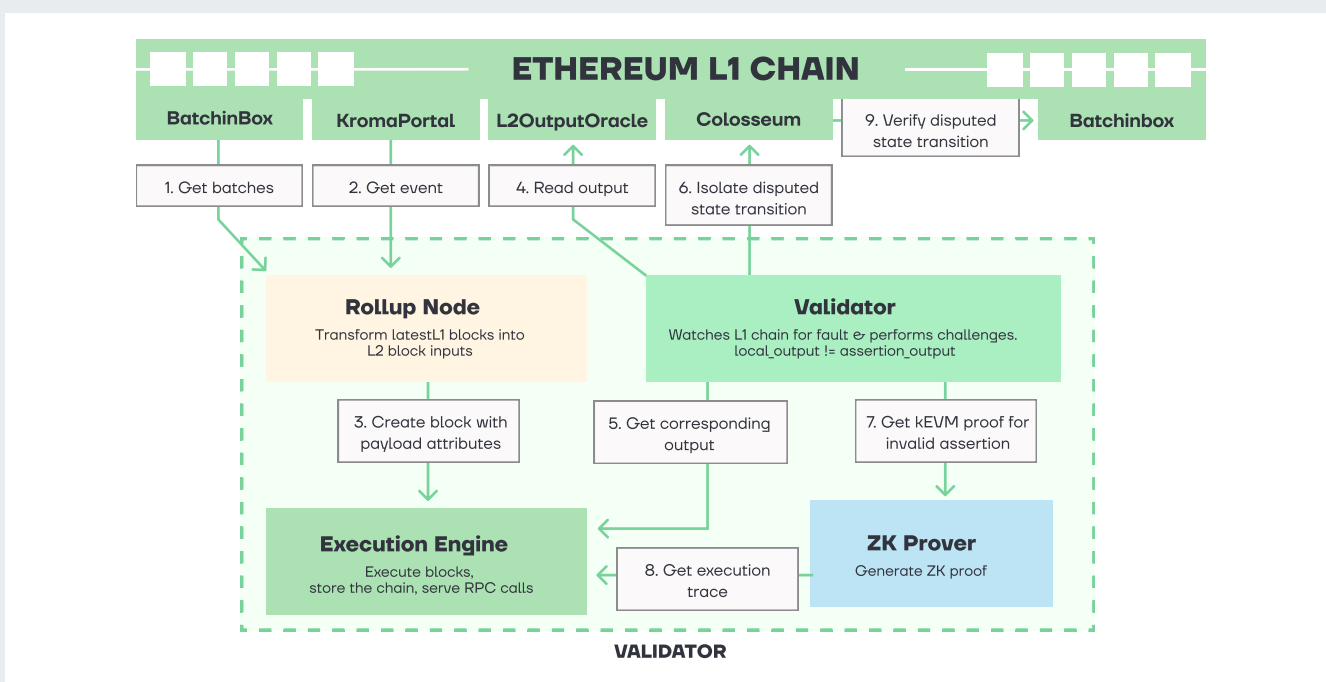


Figure 58. Validator acts as a Challenger.

Source: An Overview of Kroma's Architecture.



If a challenger suspects an output root to be flawed, the initial step involves retrieving pertinent data from two main sources: BatchInbox and KromaPortal. This data is then meticulously transformed into an execution payload, subsequently processed for block creation and state updates. By juxtaposing the output root derived from the L2OutputOracle with its locally produced counterpart, the system can verify its accuracy. Any observed discrepancies prompt the challenger to lodge a formal dispute with the Colosseum contract on L1.

Addressing such challenges necessitates pinpointing the exact onset of the discrepancy at a singular block level. The subsequent stages involve generating a ZK Fault Proof, validating this proof, and determining the rightful party based on proof verification. In an effort to localize the exact faulty block from a vast pool of blocks (typically 1,800), a systematic bisection approach is deployed. This procedure is optimized in Kroma by submitting output roots in a sequential manner, ensuring that the challenger submits the output root during the final turn, making the challenger the sole entity responsible for generating proof.

- **From OR to ZKR**

Now Kroma plans to make a transition from OR to ZKR. When a block is formed, it necessitates the generation of a ZK proof. Given the time disparity between block creation (every two seconds) and ZK proof generation, multiple provers operate in tandem. Notably, barring the first proof  $_{(i+1)}$ , subsequent proofs encapsulate preceding ones, ensuring only a single proof is requisite for checkpoint output verification. This simultaneous generation, while optimizing efficiency, may lead to resource redundancy. Kroma's design for ZKR aims to allocate resources judiciously, leveraging consensus algorithms like PoW and excluding central coordination. Proofs can be disseminated among provers via P2P networks.

There's a balance to strike between the frequency of checkpoint submissions: increased intervals result in larger public inputs, but shorter intervals elevate submission costs. This necessitates a judicious choice of checkpoint submission intervals during the transition to ZK rollup.

The transition to ZKR is streamlined when ZK proof generation becomes more time efficient. A vital phase involves using a Coordinator. Post block  $B_j$ 's challenge period, blocks are finalized promptly as checkpoint outputs undergo ZK proof validation. The entire network morphs into a ZK rollup post this challenge period, eliminating elaborate migration procedures.

In its updated form, Kroma's structure focuses on ZKR, where validators offer data outputs with accompanying validation proofs. Verification requests are initiated by L2OutputOracle via ZKVerifier upon every checkpoint output submission. Kroma's modular design is poised to accommodate ZK Proof features effortlessly, with components like ZKVerifier and ZK Prover serving both ORU and ZKR. This modular setup ensures a fluid transition.

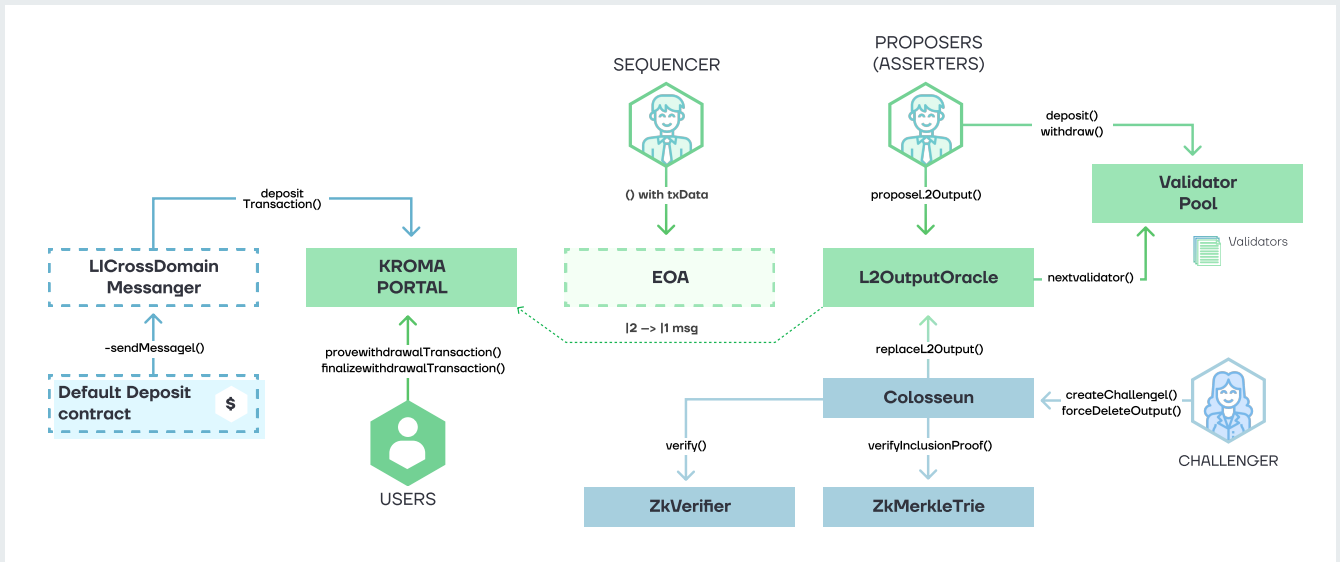


Figure 59. The system of Kroma's smart contracts.

Source: L2Beat.

And the overall architecture can be seen below:

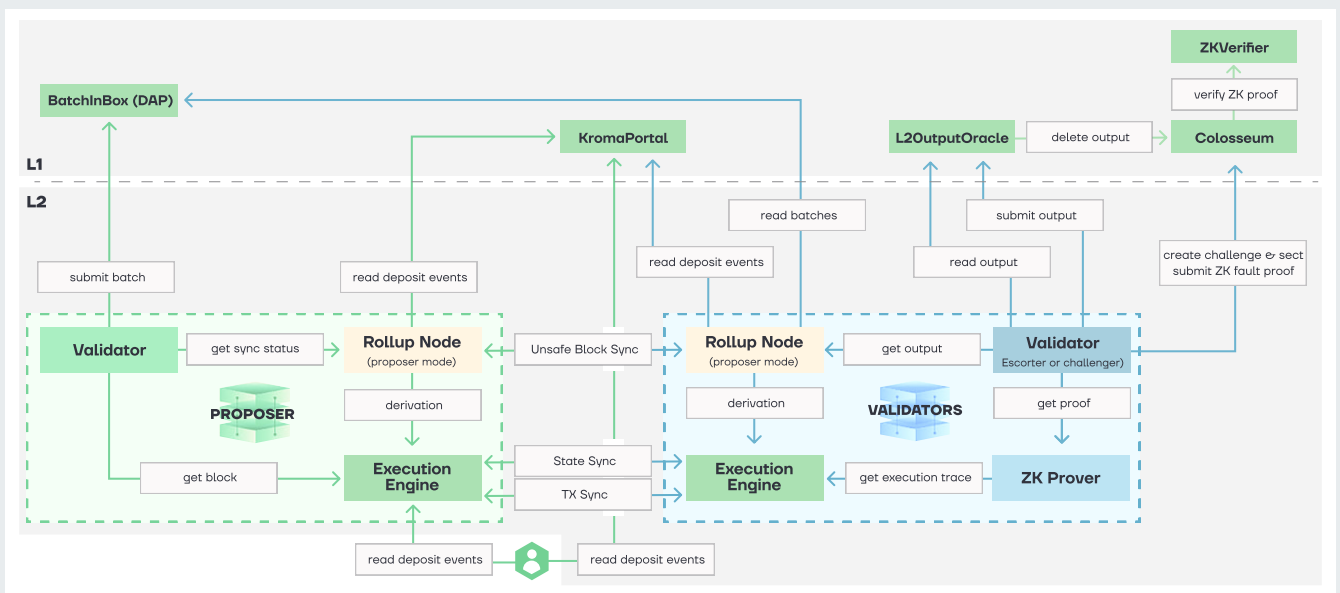


Figure 60. Overall Architecture.

Source: An Overview of Kroma's Architecture.

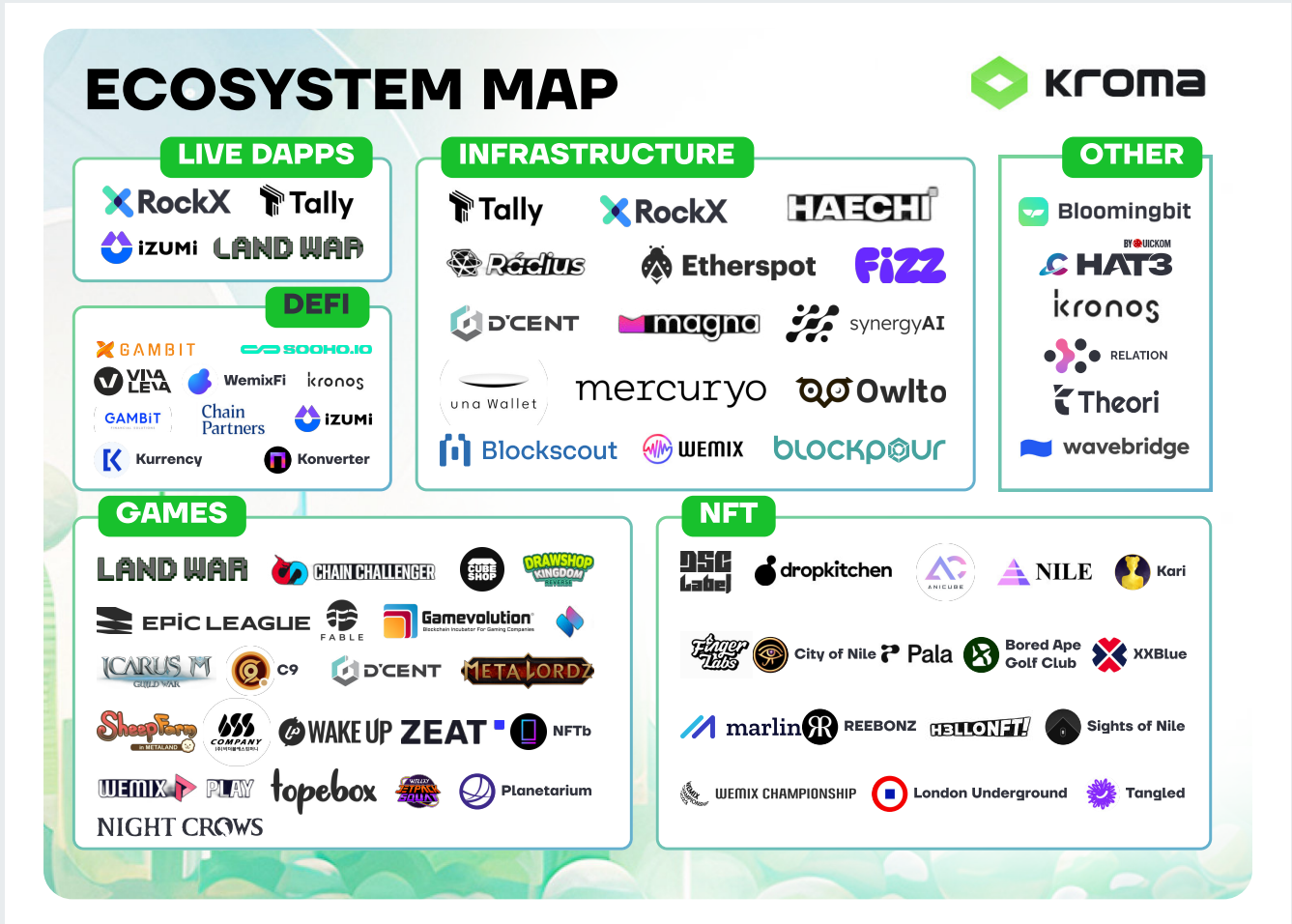


Figure 61. Kroma Ecosystem Map.  
Source: Kroma Ecosystem.

Roadmap

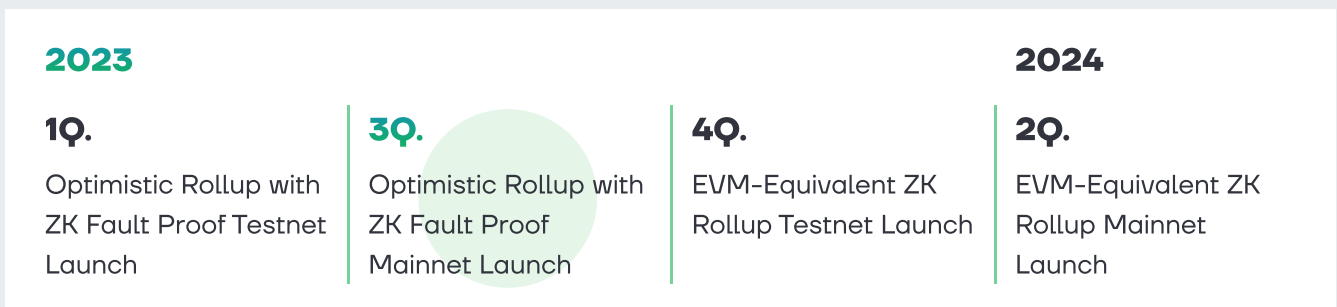


Figure 62. Kroma Roadmap.  
Source: Kroma Website.

Conclusion

Kroma is a ZKR solution based on the Optimism Bedrock framework. Currently, in its testnet phase, Kroma operates as an OR with ZK Fault Proof, utilizing a zkEVM from Scroll. The architecture involves three principal roles: Users, who make standard deposits, withdrawals, or transactions; Proposers, who collect and organize

these transactions into blocks for the main layer; and Validators, who verify blocks for accuracy and flag discrepancies. In its testnet form, while a dispute challenge mechanism is not yet active, it's still in development.

Kroma's transition plan to ZKR is rooted in optimizing the efficiency of ZK proof generation. Currently, due to the time gap between block creation and ZK proof generation, multiple provers operate concurrently. Kroma aims to strategically allocate resources, use decentralized consensus algorithms, and fine-tune checkpoint submission intervals. This transition is anticipated to become smoother as ZK proof generation accelerates. When fully transitioned, the architecture will primarily focus on ZKR, with validators submitting data outputs with corresponding validation proofs for network-wide consistency.

Kroma is designed to be an EVM-compatible Zero-Knowledge Rollup, integrating ZK Fault Proof with a centralized proposer and validator node. Validators in the system have the responsibility to challenge potentially incorrect outputs presented by their counterparts, a role termed as the 'challenger'. Challenges require meticulous examination of data from key sources like BatchInBox and KromaPortal. If discrepancies arise, a formal dispute is initiated, and a systematic approach is deployed to identify and rectify the erroneous block, leveraging ZK Fault Proof for accurate validation.

“



**Dongjoo Lee**  
CTO of Lightscale



Kroma aims to develop a universal ZK Rollup based on the Optimism Bedrock architecture.

Despite joining the Rollup development later, the Lightscale team is making a new attempt to connect the game-centric Wemix ecosystem and the Ethereum ecosystem, by developing a new rollup, Kroma, based on excellent open-source technologies like OP Stack and Scroll.

Optimistic Rollup and ZK Rollup are evolving based on their different advantages of compatibility and fast finality. While no one denies that ZK Rollup represents the ultimate form of Rollup, the time and high costs currently associated with ZK Proof generation are still constraints for users.

Kroma introduces ZK-friendly data structures and algorithms based on OP Stack and implements an Optimistic Rollup with a new form of ZK Fault Proof system using zkEVM. Kroma is the first Rollup that introduces a permissionless validator network, and the first OP stack-based rollup that establishes an active challenge system. With more than 30 validator nodes continuously submitting L2 Output since its launch in September, it has been operating stably. It has laid the foundation to smoothly transition to ZK Rollup after overcoming the limitations of zkEVM.

The Kroma team continues to research and develop for the transition to ZK Rollup. They are introducing Proto-dank sharding to significantly improve fees and throughput. Simultaneously, they plan to utilize blob commitment to overcome the constraints related to public input access caused by the way the current OP Stack stores batch data in EOA calldata. This will enhance the completeness of the ZK Fault Proof system and provide a foundation for the transition to Validity Proof in the future.

At the current stage, ZK Rollup falls short of Optimistic Rollup in terms of fees and throughput. This is primarily due to the cost and speed of proof generation, and to fundamentally address this, we are developing a new ZKP library called Tachyon. Tachyon is a general-purpose, GPU-interoperable, easy-to-use, and lightning-fast ZKP library. We plan to first replace halo2, which is responsible for the backend of scroll's zkEVM, with Tachyon and then apply it to the core folding scheme implementation for Kroma's ZK Rollup transition. In the first half of next year, we expect to release a new testnet for Kroma's ZK Rollup version, and after thorough validation, we anticipate transitioning Kroma Sepolia and Kroma Mainnet to ZK Rollup.

Lightscale is already developing Kroma and Tachyon as open-source projects and intends to make all future sources open to contribute to the development of the Web 3 ecosystem.

”

## Introduction

Manta Network is the modular ecosystem for zero-knowledge (ZK) applications. The ecosystem delivers an unparalleled experience for the next generation of web3 application development and adoption with the applied usage of zero-knowledge cryptography. As Manta is currently expanding its L2 ecosystem within its modular structure – we have added it to Zk L2s, but as you will see below Manta is developing both L1 and L2, with the main focus on its L2 - Manta Pacific. It comprises two primary components:

**Manta Pacific:** An L2 framework optimized for EVM-based zero-knowledge applications, allowing deployment in a more scalable manner with reduced gas fees using Solidity

**Manta Atlantic:** A highly efficient L1 chain that facilitates the incorporation of programmable identities and credentials in web3 through zkSBTs.

## Fundamental Components

### • Manta Pacific

Pacific presents an EVM-native Layer 2 solution featuring programmable Zero-Knowledge (ZK) capabilities. Universal Circuits enable the creation of ZK applications using Solidity exclusively. The platform leverages Celestia for data availability and the OP Stack, which supports the development of ZK applications in Solidity.

These elements collectively lead to efficient scalability and decreased transaction fees. The next phase in development aims to create a fully modular zkEVM rollup using the Polygon CDK, further enhancing the platform's capabilities. Manta Pacific will transition into zkEVM using Polygon CDK in early 2024.

### • Manta Atlantic

Manta Atlantic primarily focuses on the zero-knowledge (ZK) compliance credential layer, emphasizing real-world application and interoperability. This approach enables projects to achieve interoperable identities without the necessity of direct cryptographic involvement.

Over two years, Manta has developed a ZK circuit and infrastructure. This infrastructure incorporates a public account-based address system and a unique UTXO-based private address system termed "zkAddress". The zkAddress conceals data pertaining to minting, on-chain credentials, and off-chain identities. It stands out as a reusable, independent, and verifiable private address system, capable of supporting multiple NFTs, each with a distinct seed phase, allowing synchronization across various devices. A "Prove Key" feature lets users disclose specific zkAddress credentials without compromising privacy.

### • Universal Circuits

Manta Atlantic incorporated the initial Universal Circuits, which supported multiple zkAssets like fungible tokens and non-fungible tokens (NFTs). These circuits enabled developers to employ high-level APIs to access zkAssets.

The subsequent version, Universal Circuits 2.0, is featured in Manta Pacific, focusing on enhancing the deployment of EVM-native ZK applications. These circuits present a ZK library for developers, permitting

the simple integration of ZK functionalities into existing Solidity applications.

Universal Circuits operate as ZK-as-a-Service. Developers using Solidity can engage with Manta Pacific contracts via APIs, integrating ZK features into their applications with minimal code adjustments. Noteworthy circuit designs in Universal Circuits encompass zkContracts like zkShuffle and circuits grounded on Semaphore, developed by the Privacy Scaling and Exploration (PSE) Labs from the Ethereum Foundation.

Manta Network's ecosystem comprises two main components: Manta Atlantic, a ZK substrate framework prioritizing compliant on-chain privacy solutions, and Manta Pacific, an EVM-native execution layer targeting broader ZK application implementation. The network's adoption is evidenced by the utilization of its NPO, zkSBTs, and Manta Wallet by a considerable user base and ecosystem partners.

Manta Network's future endeavors include refining Manta Atlantic functionalities, intensifying the use of zkSBT and MantaPay for Rust developers, and launching the Manta Pacific Testnet to integrate more developers and applications. The goal is to extend the network's influence and provide comprehensive solutions for both web3 and web2 domains.

These elements collectively lead to efficient scalability and decreased transaction fees. The next phase in development aims to create a fully modular zkEVM rollup using the Polygon CDK, further enhancing the platform's capabilities. It will be the first zkEVM L2 converted from an Optimistic Rollup to a Validium using the Polygon CDK to drastically reduce gas fees through Celestia DA and increase security through Ethereum consensus and cryptographic proofs of on-chain activity. Manta Pacific will achieve modularity, decentralization, high extensibility, low gas costs, and fully EVM equivalence, while unlocking new application scenarios with novel ZK technology.

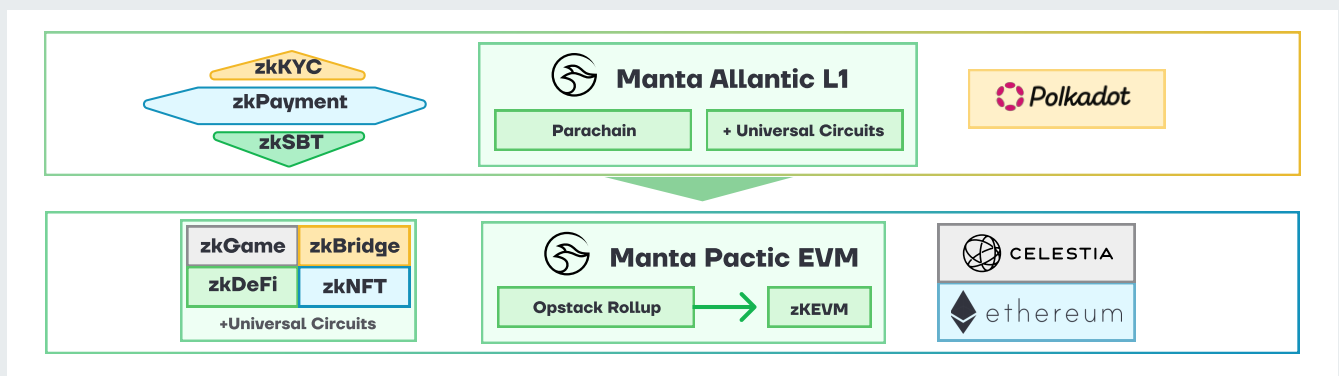


Figure 63. Manta Pacific High Level Overview.

Source: Manta Documentation.

- **Manta Network's NPO and zkSBT**

Manta Network's NPO platform facilitates the creation and minting of zkNFTs/zkSBTs. This platform utilizes Manta Network's tools and circuits to mint these items privately, using public tokens for associated costs. Manta's system allows developers to create applications without advanced cryptography or ZKP expertise. This connection simplifies the development process, particularly for mobile platforms.

Key functionalities of zkSBTs:

1. **On-chain Data Verification:** zkSBT serves as an efficient mechanism for on-chain data verification, particularly useful for mobile applications. While certain wallets, such as Particle and Unipass, provide user-friendly experiences, verifying data such as KYC information, credentials, and assets remains challenging on mobile.
2. **Decentralized Compliance:** KYC, valued at approximately \$1.6 trillion, has significant demand across web platforms. Differentiating genuine users from bots is critical. Using tools like zkBAB and zkGalxe, users can prove their legitimate status without revealing personal data or connecting to a wallet. Several applications have integrated zkSBT for this purpose.
3. **Credential Verification for On-chain Activities:** Platforms like Galxe and Cyberconnect process large volumes of on-chain activities but lack privacy. zkSBT offers a solution by allowing private verification of credentials without the need to consistently connect to a wallet. Additionally, it enables multi-chain verification.
4. **Game/Social Items:** zkSBT can function as items within games or social platforms. Examples include Ultiverse and ReadON zkSBTs, minted on the Manta chain and used across various apps.
5. **Asset Verification:** One of the primary applications for zkSBT is asset verification. With tools like Pomp, users can create zkSBTs to verify their asset holdings, similar to a confidential on-chain statement. This can be useful in both traditional and decentralized financial contexts.

- **zkAddresses and zkAssets**

A **zkAddress** in the context of zkSBT is an address that stores private SBT in Manta. Its properties include:

1. **Reusability:** The same zkAddress can be utilized multiple times without linking transactions and endangering privacy.
2. **Public Nature:** Despite being public, it doesn't expose transaction details on the blockchain.
3. **Auditability:** Transaction activities within a zkAddress can be audited using an associated proof key.

Within the framework of Manta, the zkAddress is a component of the zkAddress system, facilitating different user privileges over zkAssets.



Figure 64. zkAddress System.

Source: Manta Documentation.

This system outlines:

1. **zkAddress:** Allows the holder of its secret key to send zkAssets.
2. **Viewing Key:** Permits visibility of all transactions associated with its secret key. It can be shared for auditing or regulatory oversight.
3. **Proof Authorization Key:** Enables the holder to generate Zero-Knowledge Proofs (ZKPs) for validating transfers without the right to spend.
4. **Secret (Spending) Key:** Provides complete control over the assets it governs, i.e., zkAssets linked to the corresponding zkAddress and unspent.

From a cryptographic standpoint, ensuring the integrity and security of the zkAddress system is paramount. The system's security is rooted in:

The **spending key** being a field element with the proof authorization key derived from it using an elliptic curve point multiplication. The **viewing key** and the **zkAddress** undergo similar derivations, which are secure based on the discrete logarithm assumption.

The viewing key's derivation from the proof authorization key uses a cryptographic hash function. Due to the hash function's inherent properties, determining original inputs (preimages) from outputs is computationally infeasible.

**zkAssets** are cryptographic assets whose properties - privacy, data integrity, and access controls - are maintained using zero-knowledge proofs. These assets exhibit characteristics including diverse asset categorization, inherent privacy, selective data disclosure, and adjustable asset management policies.

“



**Victor Ji**  
Co-founder



**MANTA  
NETWORK**

Manta Pacific is the first EVM-equivalent ZK-application platform that is scalable and secure through Celestia DA and Polygon zkEVM.

Manta Network originally emerged in the Polkadot ecosystem, laying the foundation for Polkadot's zk infrastructure. From that, we expanded Manta's vision for accessible ZK to offer the ZK application layer, while simultaneously expanding to broaden our user base by entering EVM with Manta Pacific, our Layer 2. We entered the modular field early, becoming the first EVM based on Celestia and DA on Ethereum Layer 2, significantly reducing gas fees. After launching the testnet in July and the mainnet in September, we now have 127 ecosystem partners, and the mainnet TVL is one of the largest in the OP Stack ecosystem, apart from Base. However, OP Stack's longer challenge period will affect the user experience in the long term. This is why the plan to transition to zkEVM was born, as sharing the prover with Polygon can reduce the cost of proof generation and enhance interoperability.

The collaboration with Polygon CDK is just the beginning. In the future, Manta will deepen and strengthen its collaborations with more projects in the Polygon ecosystem. We maintain a developmental and inclusive mindset and will learn from the strengths of various projects to provide better infrastructure for zk applications. In ecosystem development, we will support more distinctive applications to create more opportunities for Ethereum and web3, bringing in more users. Manta's vision remains to make zk technology widely applicable. Besides scaling our ecosystem partners, we aim to enable applications that rely on zk to achieve sufficient decentralization while concealing critical information. This will open up more use cases for web3. While there may be more challenges ahead, as a project that has survived and found a place in the L1/L2 competition, we have more and more partners, a growing ecosystem, an expansion-focused team, and no reason to worry.

”

## **EVM-Compatibility and Privacy**

- **Pacific is directly compatible**

Launched in September 2023, Alpha Mainnet of Manta Pacific chain is fully compatible with the EVM, enabling it to execute standard Ethereum smart contract code directly. Because of this compatibility,



Manta Pacific integrates with various Ethereum tools, such as:

1. Libraries like Ethers.js and Web3.js.
2. Development utilities like Hardhat and Foundry.
3. Wallets like Metamask (EOAs).

Developers can employ familiar tools to construct and launch smart contracts. Furthermore, this compatibility facilitates the migration of existing Ethereum-based decentralized applications to Manta Pacific with minimal alterations.

#### • **Manta zk-SNARKs**

MantaPay utilizes a zk-SNARK named Groth16, which necessitates two key public infrastructures: a Prover key and a Verifier key. The generation of these keys is accomplished through a process known as a trusted setup. The formation of these keys adheres to specific mathematical criteria (refer to Groth '16 for a detailed explanation). The key generation process can be summarized as:

1. Random numbers, termed the trapdoor  $\tau$ , are selected.
2. This trapdoor is employed to compute several elliptic curve points, which constitute the Prover and Verifier keys.
3. The trapdoor  $\tau$  is then discarded.

The third step is crucial. While the Prover and Verifier keys don't readily reveal  $\tau$  due to the complexity of the discrete logarithm problem, possession of  $\tau$  enables the generation of deceptive proofs. This would compromise the system by allowing illegitimate transactions.

The potential to derive false proofs using  $\tau$  also underpins Groth16's zero-knowledge property: if one can conceivably produce a valid proof without knowledge of the transaction's private data, then the proof divulges no specifics about said data. The existence of  $\tau$  is necessary, but it's vital that it remains undisclosed. This is why it's referred to as toxic waste. Proper disposal of  $\tau$  ensures system integrity, and the trusted setup's purpose is to guarantee the correct formation of the keys and the secure disposal of this "waste".

# Ecosystem

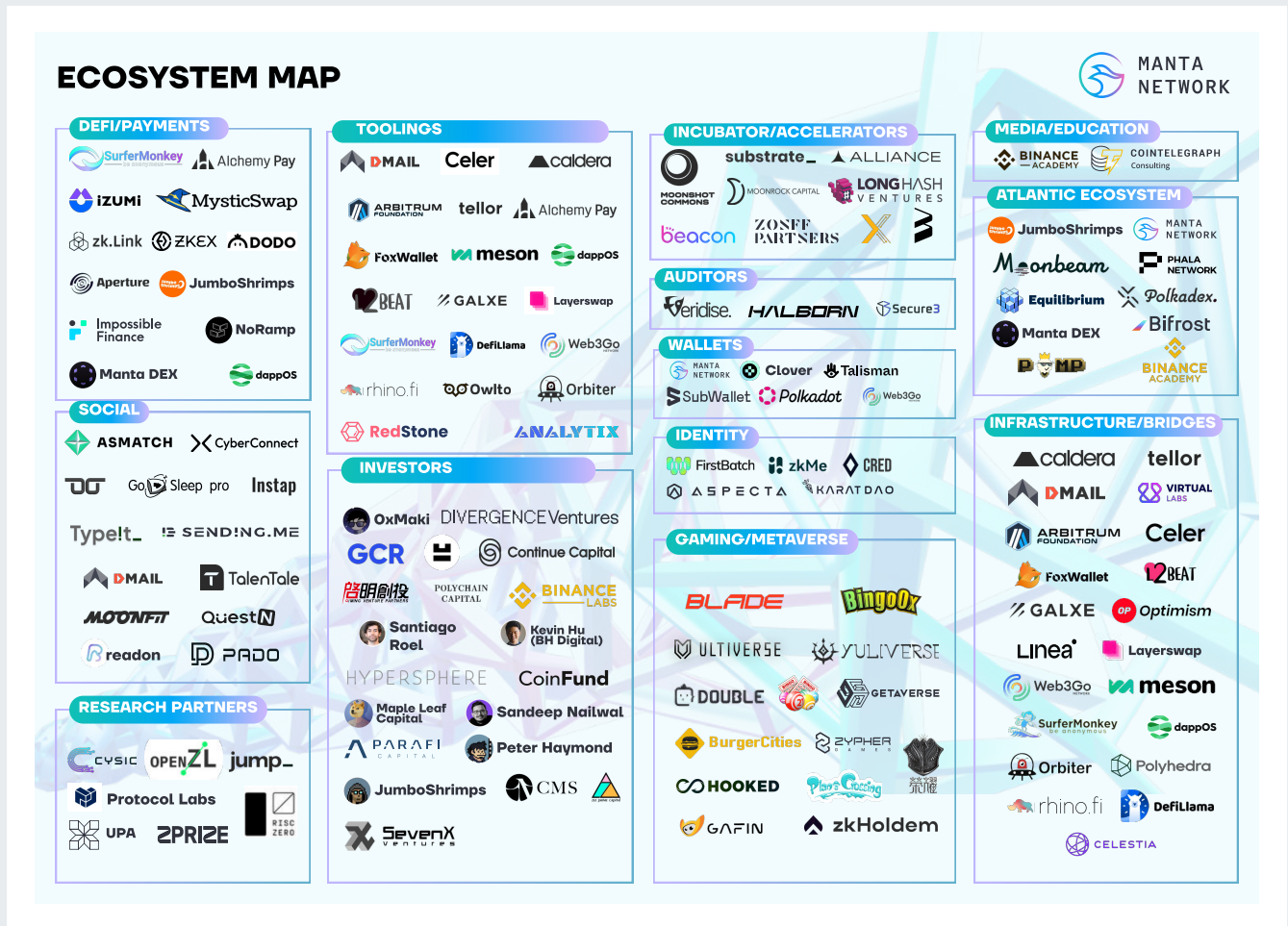


Figure 65. Manta Ecosystem.  
Source: Cryptomeria Capital.

# Roadmap

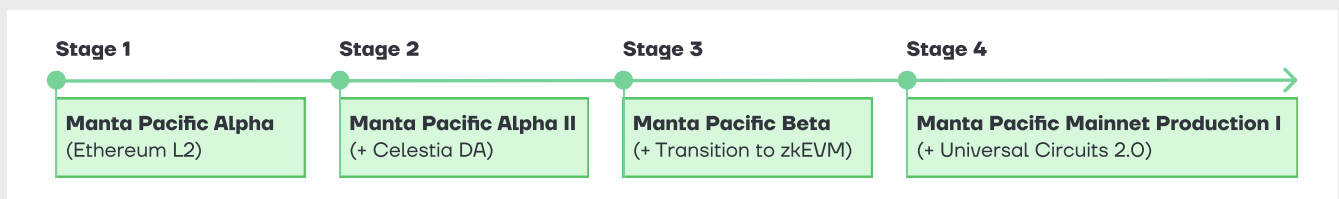


Figure 66. Manta roadmap.  
Source: Manta Documentation.

There are some upcoming updates such as:

- Universal Circuit Development and Manta SDK for them
- Manta Incentive Program IV
- Manta Network Launch
- Manta Atlantic Mainnet Launch

## Conclusion

Manta Network, a pioneering platform built on Polkadot's Substrate, is dedicated to fostering zero-knowledge (ZK) applications and ensuring data privacy in the web3 domain. Comprising two fundamental components, Manta Atlantic provides a unique Layer 1 substrate for ZK-compliant on-chain privacy, while Manta Pacific operates as an Ethereum-compatible Layer 2 framework optimized for scalable zero-knowledge applications. A standout feature of the network is the zkAddress, an innovative private address system that seamlessly integrates with both on-chain credentials and off-chain identities, bolstering transaction privacy without compromising transparency.

The network's robust infrastructure is evident in its diverse applications, from facilitating the private creation and minting of zkNFTs/zkSBTs via its NPO platform to verifying data, ensuring decentralized compliance, and even integrating into gaming or social platforms. Furthermore, the zkAddress system, underpinning Manta's framework, ensures that users maintain control, visibility, and security over their zkAssets, with the cryptographic strength rooted in established mathematical assumptions.

EVM compatibility is a cornerstone of Manta Pacific, allowing seamless interaction with familiar Ethereum tools and applications. Moreover, MantaPay's employment of the Groth16 zk-SNARK reinforces the platform's commitment to privacy, necessitating a trusted setup to ensure the security of the network. As Manta Network evolves, its focus on refining its offerings and extending its reach showcases a commitment to bridging the web2 and web3 domains, all while prioritizing user privacy and data security.

In a move driven by the desire for faster transaction finality, heightened security, and increased compatibility with Ethereum, pOx labs has chosen to migrate to the Polygon CDK. This transition leverages ZK proofs to achieve remarkably swift transaction finality, in contrast to the extended waiting periods seen in other systems, all while maintaining a high level of security through mathematical proofs. The Manta Pacific ZK dapp ecosystem requires a modular and sovereign framework, making the Polygon CDK's flexibility and adaptability a suitable choice. Additionally, Manta Pacific showcases interoperability with other chains built on the Polygon CDK through a trustless ZK bridge to Ethereum, enabling atomic Layer 2-to-Layer 2 transactions and expanding liquidity options for dapps within the Manta Pacific ecosystem.

Manta Network raised more than \$60 million backed by Polychain, Binance labs, ParaFi Capital, and Coinfund. In July 2023, Manta Network's development company pOx labs secured \$25 million in Series A funding led by Polychain Capital and Dfinity Venture Partners, bringing its valuation to \$500 million. Currently, there are more than 50 projects on Manta Pacific's Mainnet, TVL is around 12 million, and has 100,000+ addresses, made 1 million+ transactions in the first 50 days of Mainnet.

# TAKING **ZK** NETWORKING TO THE NEXT LEVEL

ZK Seasons a series of community events that feature famous speakers from the world of Zero-Knowledge with the goal of sharing experience, expanding the network, and uniting the ZK Community.



- Quality networking
- Leading ZK projects and ecosystems
- Esteemed investors
- Major conferences
- Tightly-knit community
- Hacker Spirit

Among previous speakers



[zkseasons.com](https://zkseasons.com)



# CURRENT ZK LAYER 1 LANDSCAPE

## I. MINA



### Introduction

Mina is a Layer 1 blockchain designed from first principles with zk-SNARKs at its core. Incubated by o1Labs, this unique approach results in a compact blockchain, capped at just 22 KB. Mina developers write smart contracts and provable programs in TypeScript by using the o1js library, setting itself apart as a trailblazing protocol in the space and allowing developers to embed Mina in their existing projects as a natural extension.

As an account-based ledger, Mina enables users to create state transitions by crafting transactions that meet the constraints of an account, thereby altering balances or data. Whether a transaction involves a smart contract or a simple peer-to-peer payment, it must be proved locally. Client-side proving is a unique feature of Mina which ensures that the consensus resources only have to quickly verify the transaction proofs. It also allows for composable privacy features for each smart contract and provable-program.

Mina's Mainnet has been actively operating since March 2021 and is in the final stages of testing before it's Berkeley hardfork, introducing easily programmable smart contracts & zkApps to Mainnet.

### Architecture and Fundamental Components

- **Ouroboros Samasika and zk-SNARKS**

The Mina protocol combines this state transition system with a consensus protocol Ouroboros Samasika, to construct a new state transition system. This system includes consensus verification in the update function. An incrementally computable SNARK for this system is employed, and the proofs attest to the current state being computed correctly. The blockchain summary simply consists of the state and the proof. A blockchain summary producer will just be a prover, and a full node will only need to perform proof verification to verify the blockchain correctness.

Apart from the Block Producers there are also other roles via Mina Blockchain: Snark Workers (Snarkers), and Delegators. The full cycle is: When the Block Producer wants to produce the block, the Snark Workers will sell zk-SNARKs for each transaction inside the block, so the recursive nature of blockchain will be assured. Then the BP needs to update the blockchain state via producing a zk-SNARK that can be validated by anyone. To become a block producer, you must run a full-node and MINA must be delegated to your stake pool to increase the likelihood of one's node being selected to produce a block. Wallet users delegate their MINA (aka "staking") to stake pools and in return they share the rewards of block production with the block producer.

- **zkApps**

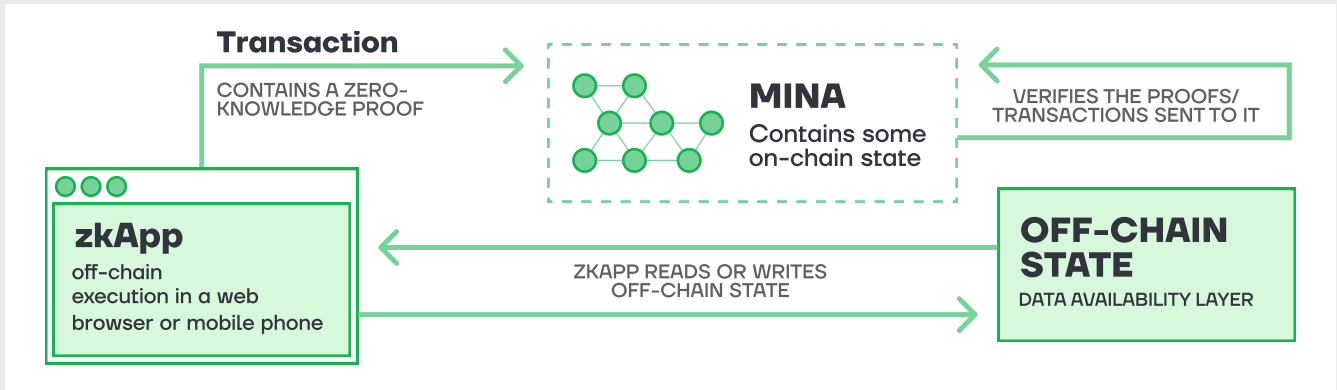


Figure 67. zkApps scheme.

Source: Mina Protocol Documentation.

Unlike many other blockchains that execute computations directly on-chain, often incurring high gas fees for running dApp executions, zkApps present a distinct approach. They enable boundless off-chain computations and utilize on-chain verification mechanisms, all under a low, fixed fee structure thereby maximising the utility of blockspace on Mina. This provides a more predictable and cost-effective environment for decentralized applications.

- **In-browser proving & verifying**

zkApps are composed of three key elements: a user interface (UI), smart contracts and provable programs; featuring Prover and Verifier functions. The Prover function operates locally in users' web browsers, executing smart contract logic while keeping private data confidential. It then generates a zero-knowledge proof of execution, safeguarding sensitive user data. This proof is sent to the Mina blockchain, where the corresponding Verifier function validates it.

Mina's off-chain execution approach empowers users to maintain control over their data, sharing only the proof of computation with the network. This ensures enhanced privacy and security in zkApps that can be tailored to the specific zkApp use-case. Furthermore, this makes Mina a leading protocol for app-chains and fractal scaling.

## **EVM-Compatibility and Privacy**

- **Mina zkVM**

Mina has achieved EVM compatibility by establishing a connection with the Ethereum Blockchain through zkBridge. This bridge is responsible for storing and regularly updating the current state proof of the Mina blockchain within a smart contract on the Ethereum Mainnet. This bridge allows Ethereum dApps to utilise Mina as a private computation layer as well as the Mina ledger state in their contract execution.

- **o1js**

Designed and developed by o1Labs, o1js (fka. SnarkyJS) is a TypeScript library for developers looking to create applications powered by zero-knowledge based on Mina Protocol. It offers a simple way to write zk-programs and is specifically designed for zk-SNARKs and zkApps. o1js is fantastic for creating domain models which address an application's solution space and because it is extensible new features can be

added as the user's needs evolve. Regardless if an application is focused on DeFi, gaming, identity, privacy or otherwise, o1js presents a natural extension to any TypeScript developer's experience. o1js provides account state fields, which are often used to store the root of a merkle tree which allows developers to verify off-chain data in zkApps.

zkOracles will provide an opportunity to include proof of web2 data in zkApps, which will be a significant step forward for web3.

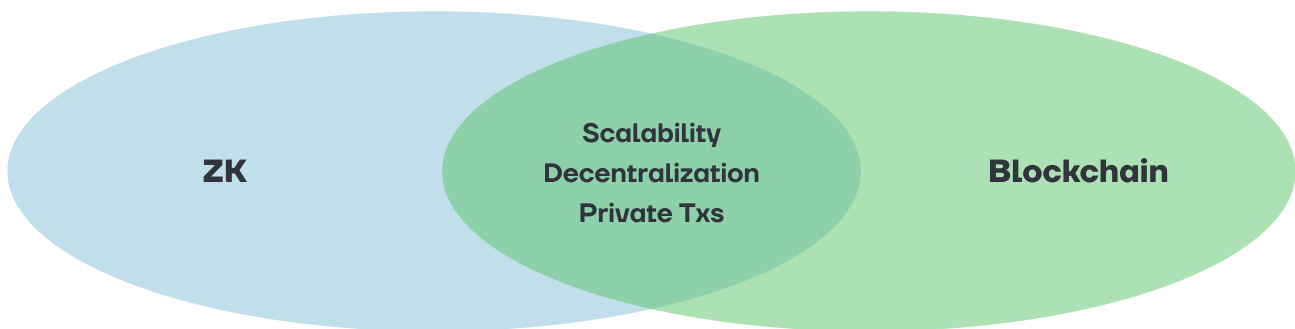


**Emre Tekişalp**  
CEO



o1Labs is a global and remote company that incubated the [Mina Protocol](#). Our team operates on the cutting edge of Web3 and zero-knowledge-proofs.

Zero Knowledge Proof technology (ZK) and Blockchains are ultimately tools to solve the trust problem. Where blockchains combine economic incentives with general purpose cryptography to create a permissionless settlement layer for value and applications; zero knowledge proofs take a purely cryptography based approach. By doing so, they trade off different pros and cons to enable new properties for developers, both to complement blockchains where they fall short, and for use cases where one might not even need a blockchain at all.



So far it looks like ZK has found a product market fit for scaling blockchains in a secure way. There's many different approaches that are being worked on, including:

- ZK rollups such as zkSync or Scroll,
- Non-ZK rollups that are starting to add ZK, such as Optimism's initiative with o1Labs and RiscZero,
- New L1 chains such as Mina and Aleo.

This is great, but I think we are only scratching the surface when it comes to what ZK can enable for blockchains and more. I think in 2024 we are going to be seeing the first practical applications that leverage ZK, for use cases such as consuming user data privately via attestations, games that allow for fairness and secrecy, ML modules that can make commitments to on-chain smart contracts, sharing of sensitive clinical trial data for medicine development and many more novel ones. And these will not be only for blockchain based applications, but also for those that do not (yet) use a blockchain. An example of this is how web3-friendly [Snickerdoodle](#) has decided to start using o1js, o1Labs' TypeScript ZK framework, and in the first phase of work, this will happen without settling the proofs on a blockchain.

I say 2024 is a breakthrough year because we now have performant and maturing development frameworks that make ZK usable by an average developer without the knowledge of advanced cryptography. Tools such as o1js and the off-chain execution of smart contracts on Mina Protocol; ZK compatible virtual machines such as o1Labs' MIPS VM or RiscZero's Risc-V engine that allow developers to use multiple existing languages; or the ongoing maturing of brand new languages such as Circom for EVM based applications, all allow for developers to add ZK to apps in production. With such powerful tools and capabilities, ZK is off to the races to "catalyze a new generation of applications" (as we like to say at o1Labs) and bring in a new wave of excitement to Web3 and beyond.



## Ecosystem

In 2023, MINA achieved significant milestones by successfully concluding two ecosystem zkIgnite Cohorts while providing grants to a total of 70+ zkApp projects. These projects can secure funding from a generous grant pool of 500,000 USDC and 500,000 MINA tokens.

Starting in October, all zkApps will undergo extensive testing on the Mina Protocol for approximately two months within the TestWorld 2.0 Track 3 environment. To achieve this significant milestone, 265 experienced node operators were carefully chosen from a pool of over 3,300 applicants earlier this year.

At least 64 verified projects will actively participate in the Mina Protocol ecosystem, as listed on the official website zkappsformina.com. Some of them have already closed early VC rounds, like KYC-enabled enterprise-ready DEX Lumina.

## Roadmap

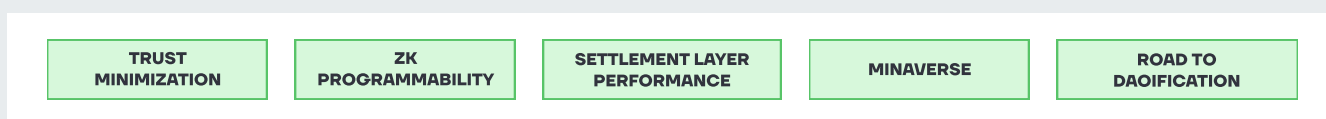


Figure 68. Mina Roadmap.

Source: Mina Protocol Documentation.

In early 2023, MINA initiated its first MIP (Mina Improvement Proposal) through on-chain voting. But they are still developing zkBridge and zkOracle, which are now longer than their initial roadmap deadlines.

- **In August 2023**, MINA concluded external security audits and promptly addressed minor bugs ahead of the TestWorld 2.0 Track 3 launch. Testworld Mission 2.0 will feature 4 tracks:
  - zkApp End-to-End (E2E) Testing (Done);
  - External Security Auditing (Done);
  - Protocol & Performance Testing (Now);
  - Preparation for the Hard Fork (Next);

In future Hard Fork, Mina Protocol will also introduce a new proof system and streamline the development and deployment of zkApps, making it a more user-friendly and efficient process. The next pivotal milestones on the horizon include:

1. Full In-Browser Nodes and Multi-Server Storage: This encompasses the development of full in-browser nodes and the implementation of multi-server storage, along with modular blockchain storage and bonded on-chain data availability as part of the strategic plan.
2. Launching zkApps on MINA Mainnet: The upcoming launch of zkApps on the MINA Mainnet after TestWorld, which is expected to bring more activity to the platform.
3. Trustless Interoperability: MINA is actively working on establishing trustless interoperability with Ethereum and zkEVM, zkOracles, and Recursive Rollups SDK for Rollups based on MINA.
4. DAO Voting on Ecosystem Funding Distribution: allowing the community to actively participate in the decision-making process for the distribution of ecosystem funding.



## Conclusion

The Mina Protocol is a groundbreaking Layer 1 blockchain technology renowned for its compact 22 KB block size, primarily due to the utilization of recursive zk-SNARKs. Launched on a Proof-of-Stake Mainnet in March 2021, its native currency, MINA, is instrumental in block production and procuring SNARK proofs. Essential participants in the Mina ecosystem include Block Producers, Snark Workers, and Delegators, working symbiotically to maintain the recursive nature of the blockchain. Mina introduces zkApps, distinguishing itself from conventional blockchains by enabling vast off-chain computations and maximising blockspace utilisation while maintaining a fixed fee structure. This approach provides a cost-efficient environment for dApp development.

Additionally, zkApps facilitate in-browser zero-knowledge proving and verification, ensuring not only enhanced user privacy but programmable privacy that each zkApp can customise to their own use-cases. Mina's connection with the Ethereum Blockchain via the zkBridge, supported by Ethereum and Mina Foundation, augments its EVM compatibility, thus widening its utility. The platform also offers `o1js`, a developer-centric TypeScript library for crafting applications with an emphasis on privacy and naturally extending any TypeScript developer's existing experience. As of 2023, the Mina Foundation's Grant pool comprises 102M MINA tokens and 19M USD in stablecoins. The MINA DAO has emerged as a proactive entity, directing the protocol's evolution and supporting ecosystem projects. With the conclusion of the zkIgnite Cohorts, over 70 zkApp projects have been funded, and these will be rigorously tested on the Mina Protocol in the upcoming months. Notably, Mina's integration with MetaMask Snaps signifies its expanding influence, positioning it among the first non-EVM chains within the MetaMask platform.

Despite some delays in the development of zkBridge and zkOracle, Mina has maintained an active roadmap, addressing external security audits and moving forward with the TestWorld 2.0 initiative. The imminent hard fork promises enhanced development capabilities for zkApps. Strategic future milestones encompass launching zkApps on the MINA Mainnet, pioneering full in-browser nodes, ensuring trustless interoperability with platforms like Ethereum, and empowering the community with DAO voting mechanisms for ecosystem funding allocation decisions. Detailed insights can be found on the MINA Roadmap.

## L2 Summer or a Predicament?

Recently, I've heard complaints from airdrop studio that many studios had invested substantial resources and transaction volume in zkSync and Linea, only to end up with nothing, inadvertently contributing tens of millions of dollars in fees to these L2 giants. As a result, these studios have become less proactive in generating transactions with the launch of new L2 solutions.

We were originally expecting a bustling L2 Summer that wouldn't need studios, but now we're seeing that, as studios gradually recede, the transaction volume and TVL of several major zkEVMs have not met expectations. When the speculators in the market withdraw from L2, no longer contributing to the vitality and dynamism of the ecosystem, a predicament of stagnation and shrinkage emerges.

## L2 Competition Through the Eyes of an Investor

From an investor's standpoint, the rationale behind investing in Layer 2 infrastructure is predicated on the belief that well-funded teams will engage in robust ecosystem competition, leading to a diverse array of applications within their ecosystems. However, the current L2 arms race primarily emphasizes technology research and talent acquisition, rather than ecosystem development. While investing in technology and talent is strategically sound, it's crucial to remember that a high-throughput, compatible Rollup without applications holds little value; it's essentially a distant dream.

## The Growth Dilemma of the L2 Ecosystem

Waiting for natural ecosystem growth takes time. If the ongoing competition in Layer 2 (L2) applications doesn't lead to a thriving ecosystem and continues to involve duplicative investments in underlying technologies, it may hinder progress.

The current ecosystem application competition on L2 is intense, making it challenging for applications to switch between L2 chains due to grant and support considerations. This leads to territorial disputes and fragmentation among L2s. Smaller L2 applications, unable to secure support, often seek financial assistance elsewhere. Which L2s have not yet revealed their ecosystem grant plans?

## The Way to Break Through: Leading L2 Projects Taking the Initiative in Ecosystem Development

We want to avoid isolating L2s, which could fragment the Ethereum ecosystem. Leveraging L2 application suites to foster diverse products and create significant applications is crucial for the entire L2 ecosystem. Unicorn companies worth over a billion dollars should take the lead in ecosystem development. For example, Starkware and Optimism have supported FOG games with the Dojo and Mud engines. Arbitrum Grants have facilitated investments, including GMX's exclusive launch on Arbitrum, rivalling dYdX in volume and user experience. Collaboration with IOSG has backed the TreasureDAO gaming platform, known as the on-chain 4399 in the industry. The launch of the Base chain by Optimism and Coinbase, based on Opstack, witnessed the rise of Friend.tech, generating over \$20 million in protocol revenue and exceeding \$20 million in TVL.



Their strategy involves leveraging the network effect to attract developers and using protocol tokens to incentivize innovation and investment. Some zkEVM L2s favor a laissez-faire approach, allowing projects to compete naturally. However, not aggressively investing in ecosystem building can create advantages in future market share and positioning. Platforms that don't invest may face developmental bottlenecks.

### The Way to Break Through, Part Two: Competition Should Embrace the Art of Alliances and Clever Strategy

In the blockchain industry, Ethereum's shift to Rollups has shifted the focus to Layer 2 (L2) networks. These networks are pivotal in scaling Ethereum and enhancing its network effect. The sector's future revolves around super applications and mass user adoption. Given the substantial investments in L2s, the question arises whether they should engage in a competitive race to develop ecosystem applications.

The role of capital in rapidly advancing the Ethereum roadmap is crucial. With billions invested, how this influences innovation in user-centric applications is a key consideration.

Moreover, the zkEVM technology is seen as a catalyst for broad innovation, suggesting that L2s should not only focus on technology replication but also explore unique solutions and creative ideas. Open-source initiatives should aim for standardization to minimize resource waste. Strategic alliances and focused investments in groundbreaking applications, like GMX and Friend.tech, are recommended for these platforms.

### The Diverse Ecosystem's Endgame - The Growth of L3 and Application-Specific Chains

Ethereum's focus on Rollups has brought Layer 2 (L2) networks to the forefront, essential for scaling and network effects. The industry is moving towards super apps and widespread user adoption. The significant investment in L2s raises questions about their role in ecosystem app development. Capital plays a crucial role in implementing the Ethereum roadmap, and how it drives user-focused app innovation is vital.

zkEVM is seen as an innovation driver, suggesting L2s should innovate beyond existing technology. Emphasis on open-source and standardization can reduce resource waste. Strategic partnerships and investment in unique applications, like GMX and Friend.tech, are encouraged.

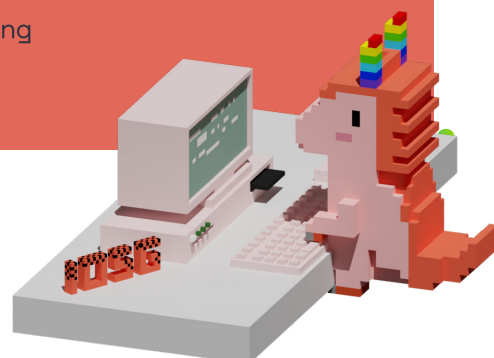
IOSG has adjusted its investment strategy, now 60% infrastructure and 40% applications, focusing on Asian team innovations in user interactions, AI apps, and social gaming. IOSG supports these teams in collaborating with L2s for ecosystem support. The article reflects personal views and is not investment advice. IOSG has investments in several L2 protocols like Arbitrum, Optimism, and Starkware.



**Jocy Lin**  
Founder



IOSG Ventures is a pioneering crypto fund founded in 2017 that invests in the future of Web3. As a thesis-driven firm, we assist founders in developing community-driven protocols that are primed to transform the crypto landscape.



### Introduction

Aleo is a privacy-first layer-1 blockchain that incorporates zero-knowledge cryptography to facilitate private and programmable transactions. Utilizing zero-knowledge proofs, it allows for the validation of information by third parties without direct disclosure of the information itself. The foundation of Aleo's operation is ZEXE (Zero-Knowledge EXECution), where users process state transitions offline, resulting in a proof. This proof is then integrated into an on-chain transaction that modifies the system's state by manipulating on-chain records. The design ensures privacy since the transactions display only the proof and not its originating inputs. Concurrently, similar to other platforms, ZEXE accommodates predefined smart contract functionalities.

### Architecture and Fundamental Components

- **Leo Programming Language**

Leo is a functional language which is statically typed and designed for the development of private applications. It complies to Aleo Instructions at a low-level. Leo necessitating predefined variable types before circuit execution. Variables must be explicitly typed upon assignment, with no provision for undefined or null values. All expressions in Leo undergo value-based passing, resulting in value duplication for function inputs or assignment right-hand sides.

- **snarkVM and snarkOS**

**SnarkVM** - A virtual machine for zero-knowledge proofs. Contrary to existing chains that keep computation on-chain and limit their scalability, snarkVM operates off-chain to introduce unlimited compute for Aleo applications.

**snarkOS** is a decentralized operating system for zero-knowledge applications. This code forms the backbone of Aleo network, which verifies transactions and stores the encrypted state applications in a publicly verifiable manner.

- **Aleo Studio and Package Manager**

Aleo Studio is an Integrated Development Environment (IDE) specifically designed for creating applications using zero-knowledge proofs in the Leo language. It aims to streamline the development process and facilitate the distribution of Leo projects within the ecosystem.

Aleo Package Manager is a system designed to manage and distribute packages for zero-knowledge circuits. It supports features like group collaborations, making it convenient for cooperative development of private applications. Furthermore, there's a direct integration between Aleo Package Manager and Aleo Studio, simplifying the process of importing and disseminating new packages.

- **AleoBFT**

Aleo utilizes third-party proving services to conduct off-chain computation and produce zero-knowledge proofs. It employs AleoBFT, a consensus mechanism that integrates elements of both proof-of-work and proof-of-stake. In proof-of-stake, transaction validation is based on a participant's stake in the network. Conversely, in proof-of-work, validators are chosen based on their capability to compute intricate puzzles.

AleoBFT mandates validators to commit their tokens and concurrently solve a succinct proof-of-work puzzle. This design aims to enhance security and scalability while mitigating centralization risks. Within Aleo, the Virtual Machine (VM) manages computational tasks, the Operating System (OS) upholds a consistent network state, and AleoBFT ensures consensus in its distributed configuration. Also, Aleo provides a comprehensive set of development tools and APIs for building privacy-centric internet applications.

## **EVM-Compatibility and Privacy**

### **• Aleo zkVM**

Aleo has privacy-first design and is not EVM-compatible. Aleo uses its own virtual machine called snarkVM and a programming language called Leo. On the privacy side Aleo uses a tailored set of pairing-friendly Twisted Edwards and Barreto-Lynn-Scott elliptic curves to perform efficient proof generation and verification.

Developers can use Leo, or directly employ AVM instructions to craft programs. Once deployed on-chain, these programs are converted into serialized AVM instructions and stored in a program registry. The R1CS representation, along with the relevant keys, can be derived from the AVM bytecode, enabling users or third-party Provers to generate transactions off-chain. Validators only need to confirm the zero-knowledge proof in the transaction, eliminating the need for program re-execution, and ensuring data privacy as input data is provided off-chain by users. The system's architecture is deemed ideal for financial applications, identity systems, on-chain games, and more.

### **• zkCloud**

zkCloud is an advanced off-chain computing environment that ensures secure, private, and cost-effective program execution with no runtime constraints. By segregating application runtime from the blockchain's maintained state, Aleo facilitates comprehensive programmability and confidentiality, alongside superior transaction throughput compared to traditional on-chain virtual machines.

The 'outer proof' stands as the conclusive output of this process, serving as the sole confirmation of any transaction's occurrence within zkCloud, even in complex applications.

Through shielded transactions, zkCloud integrates with the Aleo blockchain. These transactions interact with on-chain records, altering and updating the status of various applications or programs. Nodes and other users authenticate the zero-knowledge proofs within these shielded transactions, ensuring their authenticity without access to specific transaction particulars. With only proofs being relayed on-chain, the exposure or exploitation of transaction details becomes technically infeasible. Moreover, the efficiency of transaction throughput is significantly enhanced as Aleo nodes solely verify proofs, eliminating the need for running programs.

## **Ecosystem**

Aleo has its own grant program with \$1m of deployed capital and 15+ funded projects. There are 3 stages of this grant program:

- Ignition Grant - \$3000 - a grant for simple applications on Aleo to kick-start your development journey

- **Blueprint Grant** - \$10k-\$100k - a grant to provide a blueprint of a working application, which will be implemented into Aleo ecosystem
- **Launch Grant** - \$10k-\$200k - a grant for seasoned developers who can propose full-featured, multi-milestone projects

## Roadmap

- **2022:** Aleo releases Testnet 3, with the introduction of Provers.
- **2023:** Aleo plans to launch its Mainnet.

And there are some generalized fields of movement:

1. **Privacy-Preserving Smart Contracts:** Leveraging zero-knowledge proofs and cryptography, Aleo will introduce smart contracts prioritizing data privacy without compromising transparency.
2. **Scalability and Network Efficiency:** Aleo focuses on enhancing network performance by increasing transaction throughput, reducing confirmation durations, and optimizing resource use.
3. **Interoperability and Cross-Chain Integration:** Aleo plans to bolster interoperability, enabling communication with other blockchain platforms, thereby fostering compatibility and innovation.
4. **Enhanced Developer Tools and Documentation:** Continuous improvement of tools and resources for developers is prioritized to streamline the development process and widen community participation.
5. **Governance and Community Involvement:** Aleo emphasizes decentralized decision-making and increased community participation in pivotal protocol enhancements to ensure alignment with stakeholders' visions.
6. **Integration with Real-World Use Cases:** Collaborating with industry-specific entities, Aleo intends to highlight the practicality of its platform across sectors like healthcare, finance, and supply chain management.
7. **Research and Academic Collaborations:** Partnerships with academic institutions will be pursued to blend theoretical advancements with real-world applications, promoting sustained innovation in privacy-focused blockchain technology.
8. **Leo programming language:** The language is currently in an alpha stage and is subject to breaking changes.

## Conclusion

Aleo is a layer-1 blockchain platform that incorporates zero-knowledge cryptography to validate transactions without disclosing their specific details. Its core mechanism, ZEXE, allows for offline state transitions which generate a proof. This proof is subsequently recorded on-chain, displaying only the proof itself without the original transaction inputs. Integral to Aleo's infrastructure are: the Leo Programming Language, structured for creating applications with privacy features; snarkVM, a virtual machine handling off-chain execution of zero-knowledge proofs; and snarkOS, an operating system that maintains a consistent state of the network. Additionally, Aleo has developed Aleo Studio, an Integrated Development Environment, and a Package Manager to assist in the development and distribution of circuits based on zero-knowledge proofs.

Aleo's infrastructure does not align with the Ethereum Virtual Machine (EVM) due to its reliance on snarkVM, which caters to its specific cryptographic requirements. For its cryptographic operations, Aleo employs a select set of elliptic curves designed for proof generation and verification. Established in 2019, Aleo has initiated several testnets and received funding, including a \$200 million Series B round in 2022. It aims to release its mainnet by 2023. Objectives in Aleo's developmental roadmap encompass the creation of smart contracts with privacy features, methods to optimize network performance, refining development resources, and establishing applications in sectors like healthcare and finance.

Within its ecosystem, Aleo has instituted a grant program segmented into three tiers, addressing projects from preliminary stages to complex endeavors. Strategically, Aleo underscores the importance of decentralized decision-making, fostering increased community participation, and collaboration with academic research entities. The primary aim is to explore and apply the potentialities of blockchain technology that prioritizes privacy, bridging academic theories with practical implementations across varied domains.



# CORE DISCUSSIONS ON ZK

## I. MARKET ADOPTION

### General overview

Indeed, 2023 has firmly established itself as the definitive "Year of Layer 2" in the blockchain domain. This distinction isn't based solely on optimistic statistics, such as increased transactions and record-breaking TVL. Instead, the hallmark of this year lies in the notable resurgence and robust enthusiasm surrounding Zero-Knowledge solutions and ZK-Rollups, evidenced by the resilience of funds and user activity even during the bear market and early stages of these solutions. This surge in interest reflects a collective effort within the ecosystem to reshape the landscape and strengthen the Layer 2 infrastructure. However, even with these advancements and strides in privacy enhancement, challenges persist for ZK-Rollups and Layer 1 solutions that rely on ZKPs.

A particularly notable trend is the clear shift of users from Optimistic rollups towards active engagement with ZK-Rollups, illustrating the widespread interest across the ecosystem. Moreover, the launch timings and subsequent user adoption of the latest Layer 2 networks such as zkSync Era, Linea, Base, StarkNet, and Scroll have made a significant impact. These significant developments have emerged over a relatively short period, driven by an unwavering commitment to advancing technological boundaries.

- As per the ZKValidator 2023 Q3 report, the segment anticipated to see the most significant growth in the Zero-Knowledge fields regarding "Scaling solutions," which was identified by 42.9% of respondents. "ZK for Privacy" and "ZK & Identity" were also recognized as promising sectors, receiving 23.8% and 22.2% of the responses, respectively. Conversely, a mere 11.1% of participants predicted that ZKML would emerge as the fastest-growing segment.

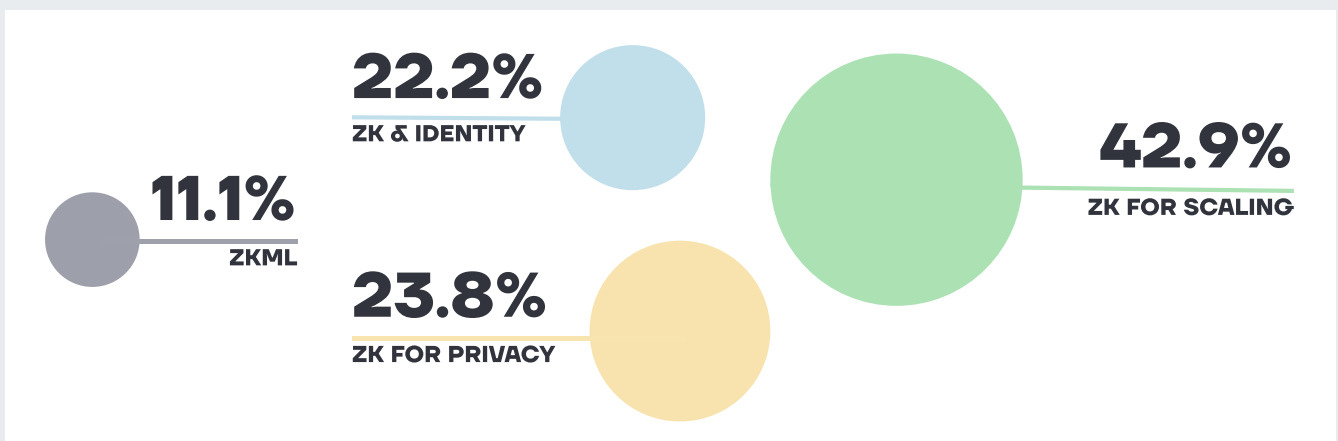


Figure 69. Potential most significant ZK fields.

Source: zkValidator: "The State of ZK Q2 2023".

Understanding privacy in the context of technological advancements and the use of Zero-Knowledge Proofs can be complex, especially in light of past precedents. Privacy and the law do not always harmoniously align, with there having been instances where legal restrictions governed the collection and use of personal data.





However, there currently exists a foundation of knowledge and practices that enable the development and use of ZKP technologies in compliance with regulatory requirements. ZKPs allow for the verification of facts and claims without revealing the underlying data, which can help protect privacy while adhering to legal standards.

Moreover, modern society is increasingly valuing the rights to personal data privacy. Many individuals and organizations acknowledge the importance of safeguarding personal information and the pivotal role of privacy in life and technological evolution. This growing interest is fostering wider acceptance of privacy-enhancing technologies, including ZKPs, provided they align with established rules and norms.

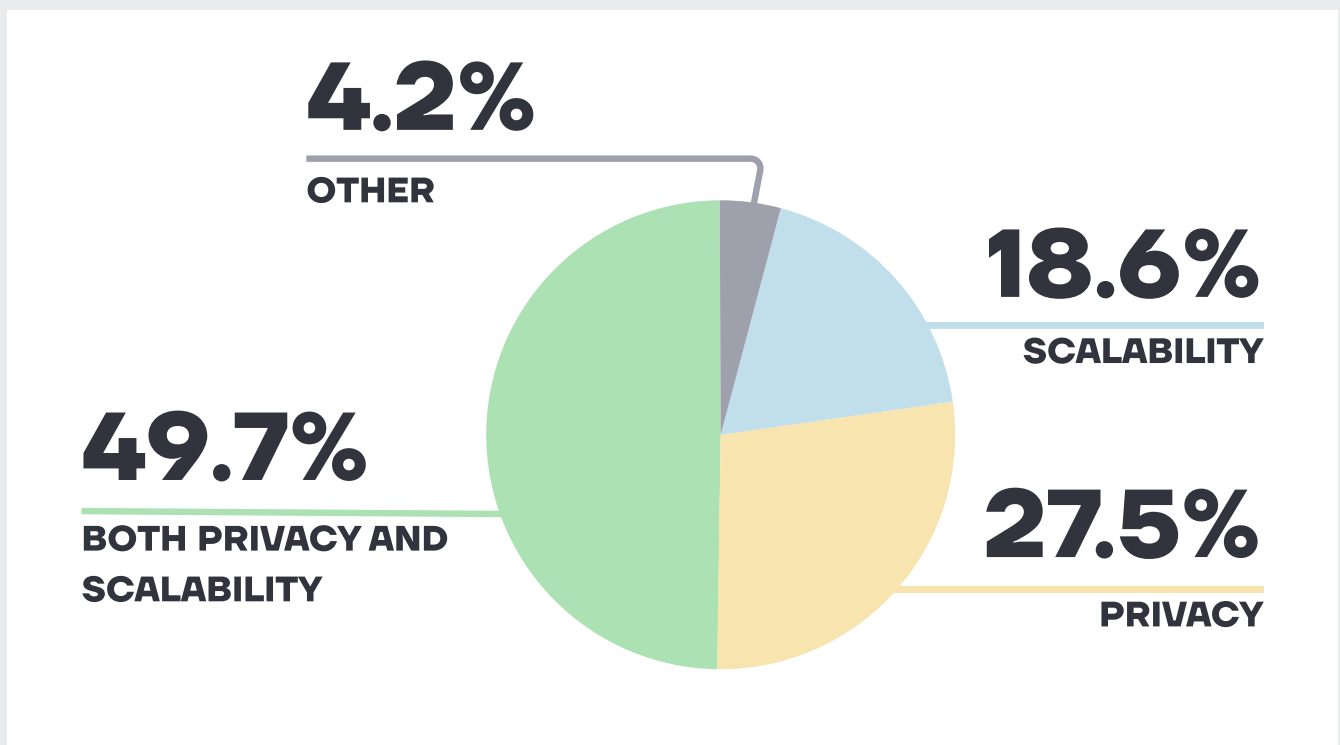


Figure 70. ZK advantages.  
Source: zkValidator: “The State of ZK Q2 2023”.

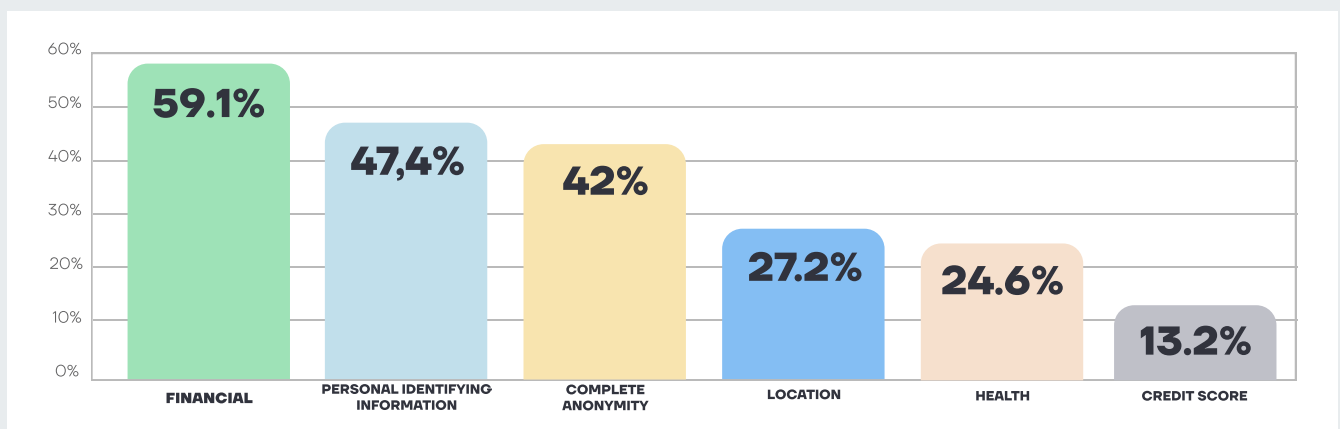


Figure 71. What type of data do you most want to keep private?  
Source: zkValidator: “The State of ZK Q2 2023”.

Despite World ID's mixed reception from Worldcoin, it has brought about a pivotal moment: the genuine recognition of ZKP technology by leading Web2 companies and the community. This acknowledgment

can pave the way for the adoption of various technological solutions, catalyzing the potential of a whole market sector and its affiliated Web2 companies.

With a strong focus on finding a consensus between transaction cost and the computational expense of Zero-Knowledge Proofs, alongside a series of technical updates, ZK-Rollup proponents are determined to provide stiff competition to Optimistic Rollups in terms of transaction cost and processing speed. Their goal is to address user demands, where the factors of cost and speed are of paramount importance. . The transaction costs associated with all ZK-rollups are fundamentally influenced by the cost of data availability. This is the reason why optimistic rollups can incur transaction costs in the range of tens of cents, even when the computational overhead is minimal.

However, it's worth noting that currently, user experience remains a more critical concern for users than privacy and security. This is understandable, as user-friendliness and platform appeal are crucial factors that can significantly influence the adoption and use of new technologies.












	NAME	SEND ETH	SWAP TOKENS
	Metis Network	<\$0.01	\$0.03
	Loopring	\$0.03	\$0.45
	Polygon zkEVM	\$0.06	\$0.79
	Optimism	\$0.07	\$0.14
	zkSync Lite	\$0.08	\$0.19
	Arbitrum One	\$0.08	\$0.23
	zkSync Era	\$0.10	\$0.31
	Boba Network	\$0.10	\$0.12
	DeGate	\$0.11	\$0.13
	StarkNet	\$0.11	\$0.34
	Ethereum	\$0.99	\$4.18

Figure 72. L2 fees.

Source: L2 fees (30.10.2023).

Using validity proofs to validate off-chain transactions is crucial in preventing unintended changes to Ethereum's state. ZK-rollups provide a robust framework that prioritizes security, decentralization, and censorship resistance. They accomplish this by refreshing the state of their underlying Layer-1 blockchains by storing compressed transaction data on the blockchain itself.

A significant benefit of ZK-rollups is their ability to drastically shorten transaction finality times. This efficiency arises because ZK-rollups require the blockchain only to verify validity proofs from Sequencers, leading to quicker transaction confirmations. Using efficient data compression techniques, they reduce user fees, rendering blockchain interactions both more accessible and cost-effective.

EIP-4844, commonly known as Proto-Danksharding, is the upcoming milestone set to be part of the major Ethereum upgrade named Cancun. The crux of lowering data availability costs for Rollups hinges on enhancing data compression and storing, especially the costs for ZK-proofs generation and circuit efficiency.

Application	Bytes in rollup	Gas cost on layer 1	Max scalability gain
<b>ETH transfer</b>	12	21,000	105x
<b>ERC20 transfer</b>	16 (4 more bytes to specify which token)	~50,000	187x
<b>Uniswap trade</b>	~14 (4 bytes sender + 4 bytes recipient + 3 bytes value + 1 byte max price + 1 byte misc)	~100,000	428x
<b>Privacy-preserving withdrawal</b> (Optimistic rollup)	296 (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient + 256 bytes ZK-SNARK proof)	~380,000	77x
<b>Privacy-preserving withdrawal</b> (ZK rollup)	40 (4 bytes index of root + 32 bytes nullifier + 4 bytes recipient)	~380,000	570x

Figure 73. How much scaling do rollups give you?  
Source: Vitalik Buterin: "An Incomplete Guide to Rollups".

## Developers activity

The cryptocurrency industry is characterized by its open-source nature, offering a unique opportunity to comprehend an emerging market with immense potential. This sector has witnessed substantial growth in developer participation, leading to the creation of innovative applications that benefit users and consequently attract more customers and developers.

Over the last 7 years, the number of monthly active developers in the crypto space has seen a significant increase, growing from 1,000 to over 22,000. In 2022, a record-breaking 61,000+ developers contributed code for the first time. This demonstrates a 66% increase in developers compared to three years ago, despite a recent decline.

The decline in developer numbers in the past year is notable, with a 27% drop since October 2022. As of October 1, 2023, there are 19,300 monthly active open source developers in the crypto sector. This decline in developer activity in the past year primarily resulted from newcomers to the field, who had been involved in crypto for less than 12 months and accounted for about 25% of all code commits.

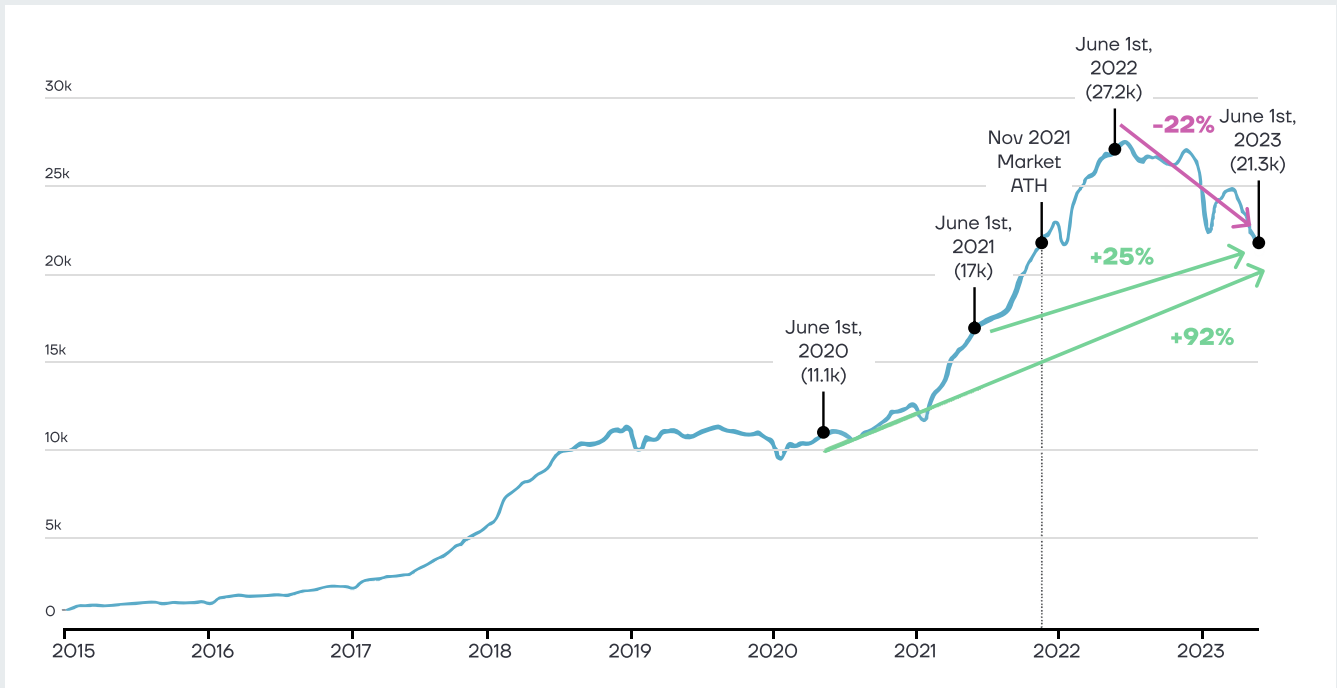


Figure 74. Number of monthly developers.  
 Source: Electric Capital: "October 2023 Developer Update".

Newcomers tend to dominate the market during periods of peak activity, whereas developers with over a year of experience (Emerging and Established developers) become more prominent during bear markets. Furthermore, developers who have remained in the crypto space demonstrate a higher level of commitment, making more code contributions on more days, and have a longer history in the industry compared to those who have left.

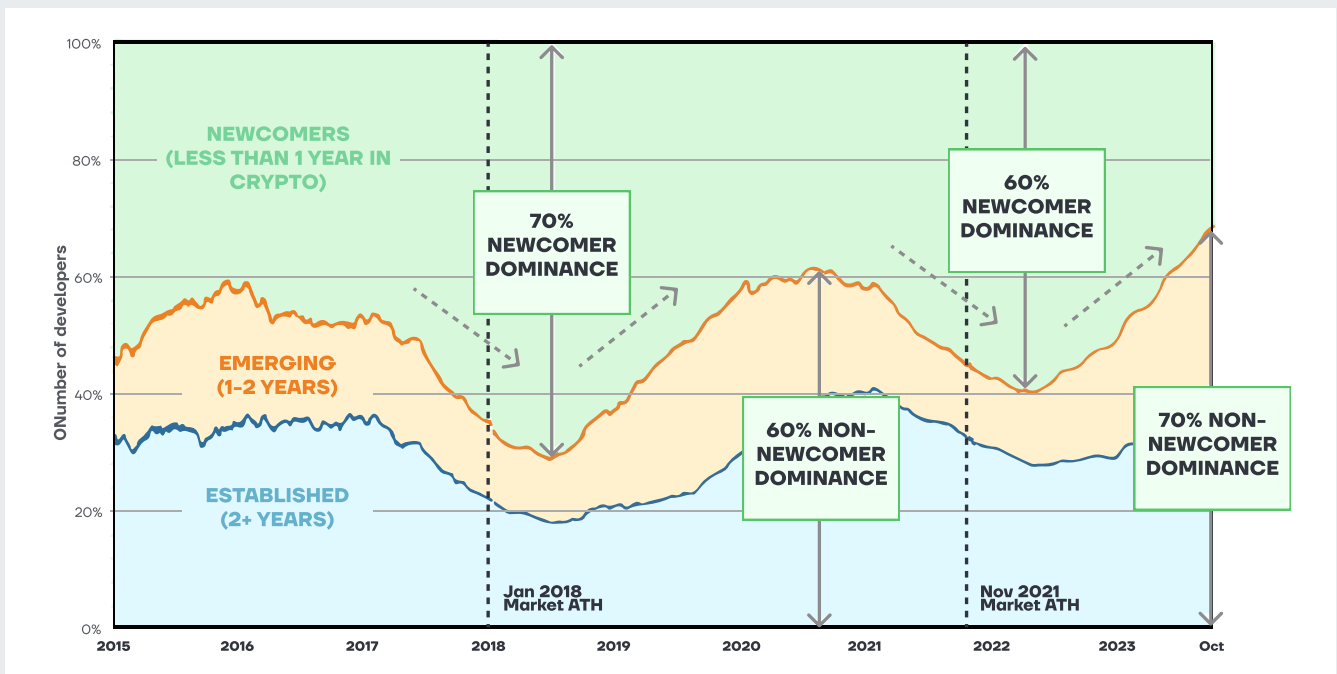


Figure 75. Number of Monthly Devs by Years in Crypto (normalized).  
 Source: Electric Capital: "October 2023 Developer Update".

Notably, several Rollup and Ecosystem projects have shown impressive growth in terms of developer engagement over the past year:

- Aztec Protocol has experienced a 168% year-over-year (YoY) growth, currently boasting 76 monthly active developers.
- Celestia has seen a 145% YoY growth, now featuring 81 monthly active developers.
- ZKSync has achieved a 6% YoY growth, with 229 monthly active developers.
- Starknet has realized a 4% YoY growth and now has 517 monthly active developers.
- These statistics highlight the dynamic and evolving nature of the cryptocurrency industry, with developers playing a crucial role in shaping its future.

“The landscape of Zero-knowledge proof technologies is expanding, with an increasing number of projects growing, gaining users, and building new networks. As it continues to advance, ZK-rollup scaling solutions are positioned to play a pivotal role in shaping the future of the Web3 and cryptocurrency ecosystems. The potential of ZK-rollup technology lies in its capacity to address some of the most significant challenges of blockchain networks, including scalability, high transaction fees, and privacy concerns. By aggregating transactions off-chain and submitting concise proofs to the main blockchain, ZK-rollup solutions facilitate faster and more cost-effective transactions, enabling decentralized finance services and smart contracts to be more efficient and accessible. Currently, numerous Zero-Knowledge protocols are undergoing active development, and it is probable that various combinations of them may be used in the future.



**ALEX MUKHIN**

Co-Founder and Managing Partner  
at Cryptomeria Capital

All ZK-proof systems share a common trait: they can convert a computation, when expressed in a ZK-friendly format and given specific inputs, into a verifiable proof. Delving deeper, modern proving systems can typically be broken down into two essential components: Polynomial Interactive Oracle Proof (PIOP) and Polynomial Commitment Scheme (PCS).

PIOP acts as a standardized protocol allowing Provers to persuade Verifiers. Concurrently, PCS mathematically ensures the procedure's security and integrity. Projects have the flexibility to tailor PIOPs to their specific requirements and select from a range of available PCSs.

Depending on the specific proof system in use, the process of generating a proof may vary. However, the primary bottleneck consistently emerges in the following areas:

## II. ZKP Hardware

### Why does hardware matter?

Discussions about rollup scalability increasingly center on the hardware and software aspects of L2 nodes. Whilst these solutions provide more flexibility in L2 operation rules, they come with a higher entry threshold due to the hardware requirements of maintaining a full consensus node, especially when compared to L1 nodes.

Rollup solutions place increased hardware demands on Verifiers because they must run both a host chain node and a rollup node. This dual-node requirement raises the barrier of entry for users who wish to fully participate in rollup transactions. Users who lack the capacity to run a host chain full node also find it challenging to set up rollup Verifiers. As a result, rollups amplify the hardware demands on Verifiers, potentially hindering the pursuit of scalability. This dual-node verification introduces another layer of complexity to discussions on scalability.

ZKP technology allows for a significant reduction in the amount of data transmitted on L1, all while ensuring data privacy and reliability through complex mathematical computations. Zcash initially pioneered this proof type. Subsequently, many L1 and L2 protocols have adopted solutions based on zk-SNARKs or other proof systems like zk-STARKs, aiming to boost data storage, security and efficiency.

Many ZKR are working on reducing the volume of published data and optimizing their own ZKP models, which should reduce the overall load on L2 full nodes and lower the entry threshold, ensuring better decentralization. Hardware improvements are also important as they enable cheaper, more complex computations related to the operation of L2 nodes.

In the context of L3 and "hyper-scalability," these aspects become even more important when considering additional layers on top of rollups, as this will lead to an increase in load on nodes - which are already expensive to begin with. To maintain low fees and a reliable environment for users - as well as to move away from centralized Sequencer and Prover/Validator solutions - it is necessary to address these problems as concisely as possible.

### Current Challenges

There are two prominent zero-knowledge proofs: zk-STARKs and zk-SNARKs. When it comes to on-chain verification, zk-SNARKs offer a notable advantage in terms of gas efficiency. Additionally, zk-SNARK proofs are significantly smaller, making them more cost-effective to store on the blockchain.

There are two prominent zero-knowledge proofs: zk-STARKs and zk-SNARKs. When it comes to on-chain verification, zk-SNARKs offer a notable advantage in terms of gas efficiency. Additionally, zk-SNARK proofs are significantly smaller, making them more cost-effective to store on the blockchain.

The core technology and cryptographic components of zk-SNARKs have been recognized since the inception of Zcash, boasting an established codebase and a robust developer community, whereas zk-STARKs remain in their infancy, striving for broader adoption.

However, STARKs are touted as a post-quantum resistant proof system and eliminate the need for a trusted setup, in contrast to non-PQ SNARKs that grapple with the necessity of such a setup. Nonetheless, ongoing experiments with PQ-SNARKs and hybrid SNARK/STARK schemes hint at the potential for enhanced security.

	ZK-STARK	ZK-SNARK
<b>Complexity - Prover</b>	$O(N * \text{poly-log}(N))$	$O(N * \log(N))$
<b>Complexity - Verifier</b>	$O(\text{poly-log}(N))$	$O(1)$
<b>Proof size</b>	45KB-200KB	~ 288 Bytes
<b>Post quantum resistance</b>	Yes (hash function based)	No
<b>Trusted setup</b>	No	Yes
<b>Zero Knowledge</b>	Both	Yes
<b>Interactivity</b>	Interactive or non-interactive	Non interactive
<b>Developer documentation</b>	Limited - but expanding	Very well documented

Figure 76. STARKs and SNARKs differences and tradeoffs.  
Source: OxMonia: "Hardware Review".

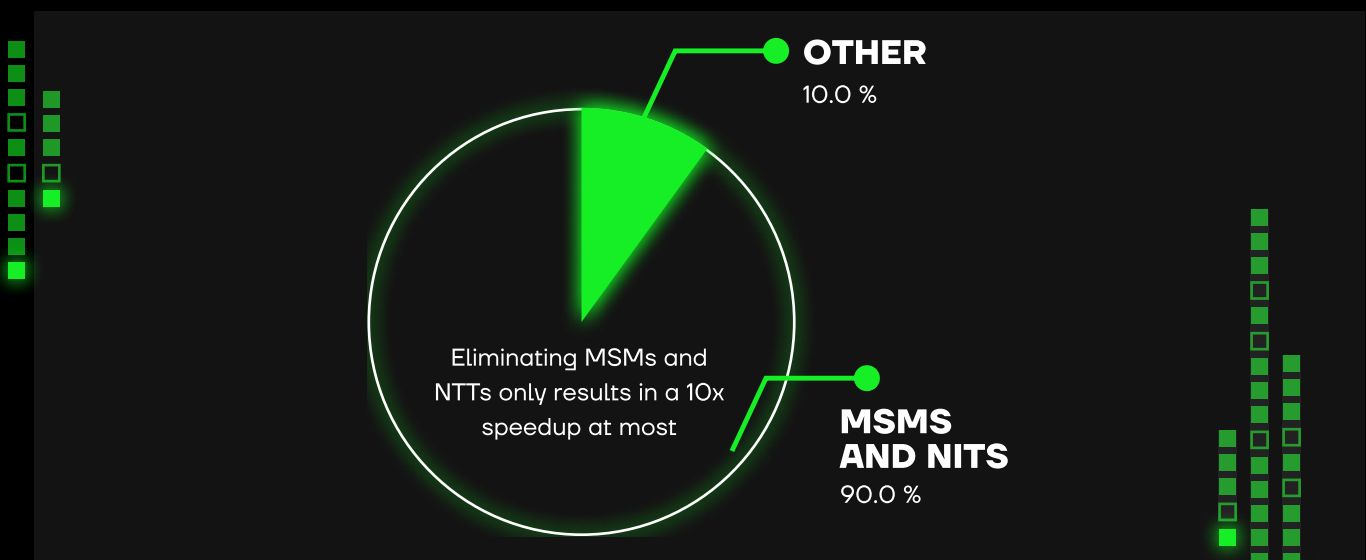


Figure 77. Amdahl's Law.  
Source: Figment Capital: "Accelerating Zero-Knowledge Proofs".

1. Multiplications involving large vectors of numbers, encompassing both field and group elements. This includes variable-base and fixed-base multi-scalar multiplications (MSMs).
2. Number Theoretic Transforms (NTTs) or Fast Fourier Transforms (FFTs) and Inverse FFTs enable a more efficient evaluation of polynomials with fewer computational requirements.
3. Additionally, other vital computational components exist. For instance, witness generation plays a pivotal role in preparing the requisite data for a ZKP. In STARKs, the hashing system's efficiency frequently becomes the main bottleneck due to its vital role in upholding security and integrity.

Computing MSMs is the most time-intensive task, with the bulk of the remaining computational effort largely falling on FFTs. While both MSMs and FFTs naturally demand significant resources, various strategies and methods exist to boost their performance.

Nevertheless, the selection and setting of different Proof systems (Marlyn, Plonk, Plonky2/3, Halo/Halo2, Groth16, Stark, etc) and PCSs (KZG, FRI, IPA, etc) can significantly influence the workload distribution between FFT and MSM computations, as well as add new challenges for ZKPs.

Algorithmic enhancements, such as the bucket method for MSMs and NTTs for polynomial evaluation, have played a significant role in improving ZK proving times. However, to achieve even greater improvements in ZKP performance, it is essential to optimize the underlying hardware.

## Hardware Solutions

There are four main hardware technologies commonly used to accelerate ZKP processes:

### 1. GPU (Graphics Processing Unit):

- GPUs constitute a large supply in the current hardware market, making them accessible and prevalent.
- Originally designed for graphics rendering, their parallel architecture is useful for various high-performance computing tasks.
- Parallelizing MSM calculations suits their multi-core design, making them common for zk-SNARKs.
- Example: Nvidia RTX 4090, a high-performance gaming GPU.

### 2. FPGA (Field Programmable Gate Array):

- FPGAs are versatile semiconductor devices that can be programmed for specific digital functions - offering high customization.
- Programming with HDLs allows for greater performance.
- FPGAs are competitive in power efficiency, yet have a steep learning curve.
- They can be reprogrammed without the need for a new chip.
- Well-suited for tasks like FFT, crucial for zk-STARKs and Plonky2/3 computations.
- Example: Xilinx U55C FPGA from the Alveo family, based on 16nm technology.

### 3. ASIC (Application Specific Integrated Circuit):

- ASICs are specialized integrated circuits designed for specific tasks. They are often used in cryptocurrency mining.



- They offer high efficiency for predefined tasks but are less flexible for modification.
- ASICs provide excellent performance and energy efficiency, as they can be precisely tailored towards specific applications.

#### 4. CPU (Central Processing Units):

- CPUs are versatile and cost-effective but have lower performance compared to specialized hardware.
- They can only handle operations sequentially, which limits their use in many applications.

Depending on specific application needs, including ZKP acceleration, each hardware technology caters to distinct purposes. Some privacy-focused applications and Layer 1 networks can perform ZKPs using CPUs for smaller proofs. Yet, when it comes to more complex ZKPs, hardware acceleration becomes crucial, rendering CPUs inadequate.

Column Name	GPU	FPGA	ASIC
Development cost	low	medium	high
User Cost	medium	high	low
Development flexibility	high	medium/high	low/medium
Energy Efficiency	low	medium/high	high
Potential performance	high	higher	much higher
Time to Market	high	medium/low	low
Suppliers	Nvidia, AMD, Intel, etc.	Intel, AMD, Lattice, Macrosemi, etc.	Self-desian
Use Cases	ZK Bridges, ZK L1s, ZK Rollups, ZK Oracles	ZK Bridges, ZK L1s, ZK Rollups, ZK Oracles	ZK Bridges, ZK L1s, ZK Rollups, ZK Oracles

Figure 78. Hardware comparison.

Source: Amber Group: "The Need for Speed: Zero Knowledge", Figment Capital: "Accelerating Zero-Knowledge Proofs".

Within hardware-driven ZKPs, multiple avenues are under exploration to boost performance and efficiency. GPUs, while suitable for parallelization, have fixed architecture limitations. Although FPGA technology is programmable, it introduces hurdles in team coordination and certain bottlenecks. Some pioneering efforts are taking FPGA acceleration a step further by creating FPGA servers and clusters to bolster memory and parallel computing, yielding promising results.

While ASICs provide unparalleled ZKP generation performance, their production hinges on ZK stabilization due to the substantial time and investment involved. An intersection between FPGAs and ASICs is taking shape, as FPGA firms explore the development of specialized components tailored for ZK operations. Meanwhile, flexible ASICs are being considered to target various cryptographic operations while maintaining adaptability.

Ultimately, ASICs are poised to provide the most potent ZKP acceleration. In the interim, FPGAs are expected to serve computationally intensive ZK use cases due to their programmability, even outperforming GPUs in certain applications. Advancements in both ZKP proving schemes and hardware are paving the way for a transformative era in Web3. By tackling computational bottlenecks, they hold the promise of enhancing scalability, privacy and interoperability.

In 2023, the ZK-Rollup ecosystem is experiencing a marked acceleration in technical upgrades. This trend includes the launch of new zkEVMs and SDKs (Kakarot, AVM, ZK Stack, Polygon CDK), new ZKP schemes (Plonky3 from Polygon, Boojum from zkSync, Lasso and Jolt from a16z, etc), the delegation of certain components of ZKP scheme execution (Loopring → Taiko, Manta → Polygon), and the introduction of multi-rollup architectures built on top of existing ZKR solutions and ZKP based Layer 1 (StarkNet, Polygon, Mina, zkSync, etc).

These crucial advancements are leading to varied requirements in both overall architecture and hardware solutions. Consequently, a rapidly expanding market for hardware and software is emerging, focused on bolstering the reliability and stability of Rollups.

The most popular ZK Hardware projects are listed below.

**Hardware Acceleration**

Figure 79. Hardware acceleration.

Source: Cryptomeria Capital.

“

**Leo Fan**  
Co-founder

Cysic designs hardware to accelerate zero-knowledge proof generation.

Cysic is currently working on realtime ZK proving. Realtime ZK proving means the ZK proof generation for the majority ZK circuits can be done within milliseconds. This vision can be achieved using a hybrid hardware system, consisting of FPGAs and ASICs, where the ASICs computes the major components, like MSM and NTT, and the FPGAs take care of the long-tail operations.

”

### III. ZKML

#### About ZKML

Zero Knowledge Machine Learning (ZKML) is a technology that facilitates calculations on encrypted data without revealing the actual data. The main goal of ZKML is to reduce the risk of leaking confidential information during the training process of machine learning models. Traditionally, when training a model, personal data could be used to build accurate models. However, this has been shown to potentially compromise data confidentiality and privacy.

With ZKML, data can be encrypted and processed so that the model is trained without revealing the data itself. This ensures the confidentiality of personal data, diminishing leakage risks — a significant advantage over traditional ML model training methods.

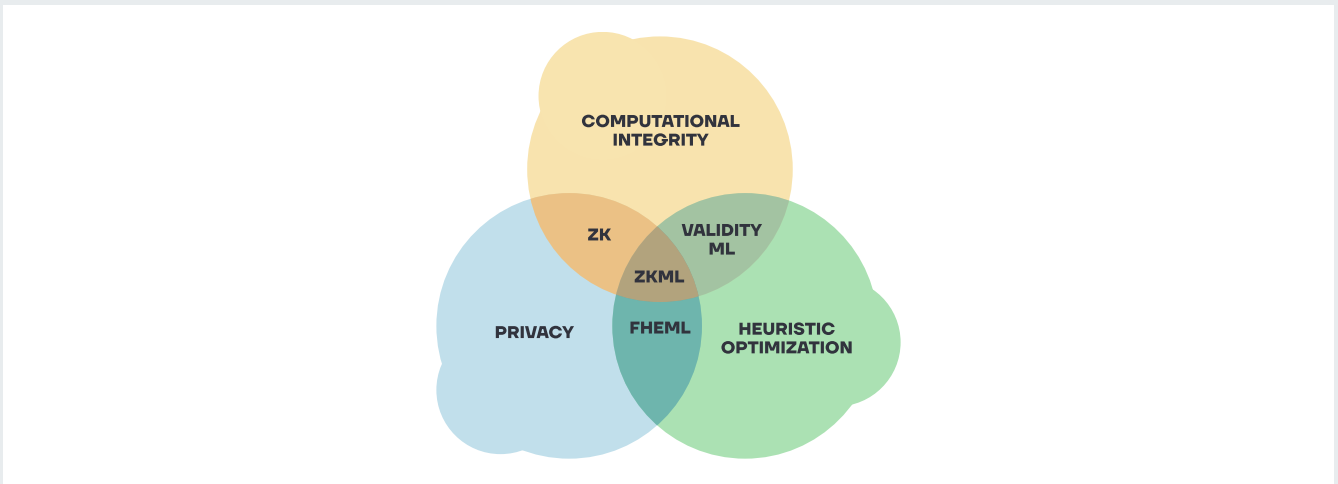


Figure 80. ZKML Venn Diagram.

Source: Worldcoin: "An introduction to zero-knowledge machine learning (ZKML)".

ZKML addresses a variety of practical challenges, such as training models on encrypted data that must remain confidential. This is especially useful for dealing with sensitive data such as medical records or financial records. ZKML can also be used for real-time data analysis. This proves particularly beneficial in financial technology, where swift and precise calculations are crucial.

#### Use Cases of ZKML

A distinctive application already in practice involves using ZKML for the privacy or encryption of AIGC. The ZKML AIGC-NFTs standard extends the ERC-721 token standard, which is tailored for AI Generated Content. This standard includes a new mint event and a JSON schema for AIGC-NFT metadata. Additionally, it incorporates ZKML capabilities to enable verification of AIGC-NFT ownership. In this standard, the **tokenId** is indexed by the **prompt**.

EIP-7007:

- mint event and a mint function for minting AIGC-NFTs
- verify function to check the validity of a combination of prompt and proof using ZKML techniques
- The **enumeration extension** is OPTIONAL for EIP-7007 smart contracts. This allows your contract to publish its full list of mapping between **tokenId** and **prompt**, as well as make them discoverable.

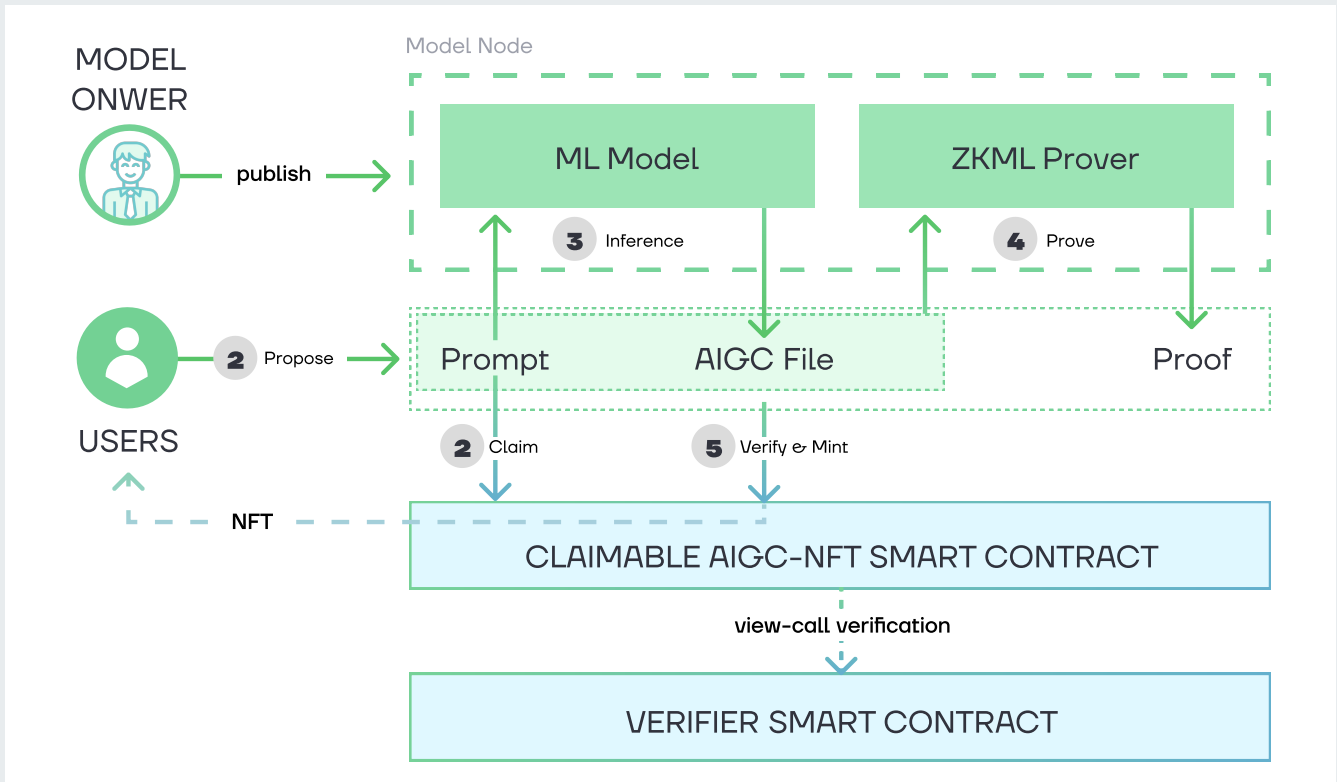


Figure 81. ZKML AIGC-NFTs.

Source: EIP-7007.

**Privacy-Preserved Model Evaluation:** With ZKML, entities can assess a machine learning model's performance without revealing its parameters. This enables potential buyers to evaluate the model's efficacy using a chosen test set prior to acquisition. Such a methodology can be applied in decentralized machine learning competitions or when conducting medical diagnostics on private patient data, ensuring only the concerned patient knows the result.

**Computational Integrity in Machine Learning:** In the context of Machine Learning, ZKML provides a means to verify the accurate execution of specific computational processes. For instance, automated trading algorithms might employ ZKML to affirm that they've implemented certain functions. Additionally, ZKML finds applications in advanced financial protocols, AI-driven reputation systems, and in ensuring contract-level compliance within protocols. ZKML also aids in ensuring that a particular output stems from a defined model-input pairing, enabling machine learning models to operate beyond the primary chain. Notably, collaborations are underway with financial aggregators to explore these capabilities.

**Machine Learning as a Service (MLaaS) Verification:** ZKML can be employed to verify that a service provider genuinely offers the model they claim.

**On-Chain Model Verification:** Within blockchain and distributed ledger frameworks, ZKML can facilitate the secure and confidential validation of machine learning models. Such a mechanism can augment the reliability and transparency of decentralized systems and contracts, which incorporate artificial intelligence components.

**Legal Discovery and Audits with Machine Learning:** ZKML can be employed for audit and legal discovery functions without compromising confidential data. This allows auditors and legal professionals to confirm the precision and compliance of machine learning models without direct access to the underlying data. Furthermore, such a methodology can be extended to smart contracts, with zk-proofs ensuring that a contract adheres to set parameters or conditions.

**ZK KYC:** This facilitates the verification of an individual's identity against their provided ID, ensuring that the ID number is not listed on any sanctions lists. Whilst this technology is available, it may not be accepted by regulators who currently require banks to 'know' their clients or 'just verify' that they are not on a sanctions list. This is uncharted territory for regulators, and precautions are essential to deter unwanted actors from exploiting decentralized projects.

**Fraud checks:** Smart contracts or abstracted accounts incorporate a ZKML fraud spam to detect unusual behaviour. This means that a system can be devised using zero-knowledge machine learning techniques to detect and counteract fraudulent or 'spammy' behavior by analyzing activity patterns and contrasting them with established patterns of such behavior.

**Making DAOs Autonomous:** zk-SNARKs technology allows for the execution of complex computations in a way that preserves the privacy of the input data, making it suitable for use in situations where sensitive information needs to be protected. Machine learning algorithms can be integrated into this technology to promote advanced decision making, assessments, and communication systems that are more efficient and accurate. Such capabilities might prove crucial for future internal DAO dynamics.

**AI Oracle Proof:** ZKML can be integrated with on-chain AI, while versions capable of handling GPT-2 already exist. Should a high-performance solution for GPT-5 ZKML be developed in the future, it could pave the way for various styles of AI Oracle Proof.

## ZKML Challenges

**Operator Limitation:** The current version of EZKL only supports a subset of the 1500+ ONNX operators, limiting the range of model variants that can be converted into zero-knowledge proofs. However, the system is continuously refined to accommodate more operators.

**Model Intricacy:** The intricacy of machine learning models, alongside their parameter count, influences the viability of creating zero-knowledge proofs. Although no strict parameter ceiling exists, intricate models necessitate extended computational duration and resources for proof generation.

**Training Consideration:** Compared to conventional methods, implementing ZKML for training introduces significant time and cost inefficiencies. Whilst future advancements in proof systems may improve training feasibility; a cost-benefit analysis remains crucial.

**Scalability Concerns:** Creating zero-knowledge proofs for machine learning requires careful optimization and a deep understanding of the relationship between Prover duration, Verifier duration and proof dimensions. Enhanced comprehension of these factors will further the scalability of ZKML methodologies.

## ZKML Projects

### EZKL

**ezkl** is a library and command-line tool for doing inference for deep learning models and other computational graphs in a zk-SNARK (ZKML). It enables the following workflow:

1. To define a computational graph, such as a neural network (or any set of arbitrary operations), in the same manner as one would in PyTorch or TensorFlow.
2. Export the final graph of operations as an **.onnx** file and some sample inputs to a **.json** file.
3. Direct **ezkl** towards the **.onnx** and **.json** files to generate a zk-SNARK circuit with which you can prove statements such as:

"I ran this publicly available neural network on some private data and it produced this output"

"I ran my private neural network on some public data and it produced this output"

"I correctly ran this publicly available neural network on some public data and it produced this output"

Projects, such as ZKonduit, view ZKML as the solution to endowing the blockchain with "eyes", enabling smart contracts to make judgments, act as one-person oracles, and generally facilitate scalable on-chain data integration. The use of ZKML oracles offers a simpler, faster, and more efficient way to transfer off-chain data to the blockchain - greatly increasing the potential for data to be brought on-chain. Additionally, ZKML has the potential to empower 'smart judges' to interpret ambiguous events.

Other projects that are using ZKML in their product are shown below as a part of the ZKML map.

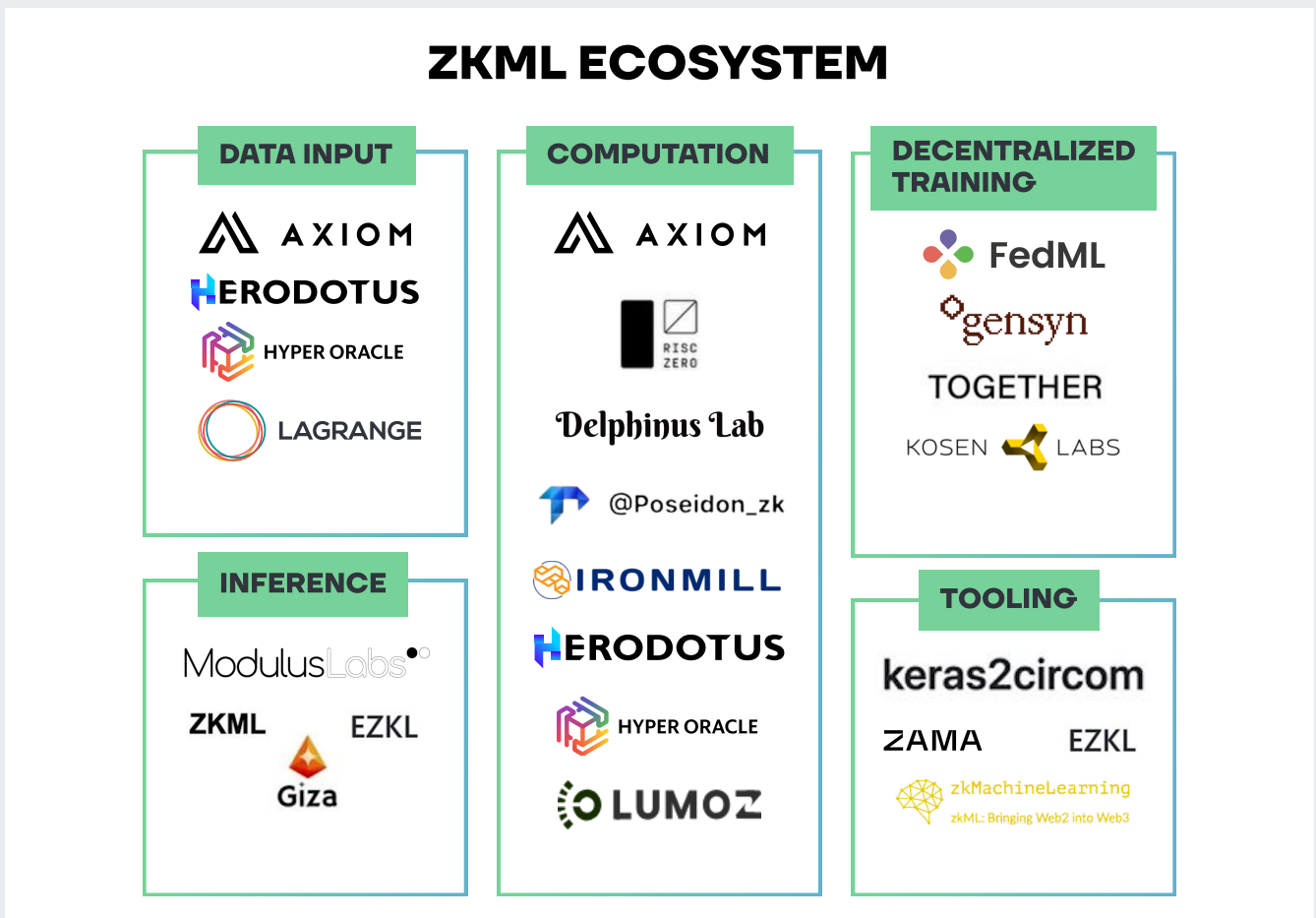


Figure 82. zkML Ecosystem.  
Source: Cryptomeria Capital.

As ZKML is a new concept that is still in early phases of development - limited information has been documented. However, in the future, ZKML will find its place in different fields, ensuring data security and facilitating the safe training of ML models.

## IV. DECENTRALISATION OF THE SEQUENCER

### About Sequencers and Validators

Sequencer plays the role of ordering Layer 2 transactions and posting these ordered transactions to the Data Availability layer, thereby committing to the content of Layer 2 blocks, or broadcasting Layer 2 blocks (e.g., zkSync, StarkNet). It is important to note that to "change" the state root is not within Sequencer's scope of responsibilities.

The Validator is responsible for selecting the Layer 2 block (from either the DA or directly from a Sequencer) and computing the new L2 state root. To perform this task, the Validator needs to determine which transactions within a block are valid. Once the Validator has computed the new L2 state root, it must generate a corresponding zkProof and post it back to Layer 1.

In cases where the Sequencer fails to post the L2 block to the DA, the Validator is required to post the state-diffs to the DA to enable the reconstruction of the full Layer 2 state. If the Validator posts an invalid state root, the Layer 1 contract will reject this state root, as it can determine that the new state root is not a result of the valid computation of the L2 block from the Sequencer.

Ultimately, only the L1 contract has the authority to conclude the operation and publish L2 state roots as being valid. In theory, a malicious upgrade of the L1 contract could enable it to accept such fraudulent state roots, underscoring the importance of the trustworthiness and security of the L1 contract in the Rollup ecosystem. However, current Sequencer models present other issues that are equally significant and pose challenges for ZKR protocols.

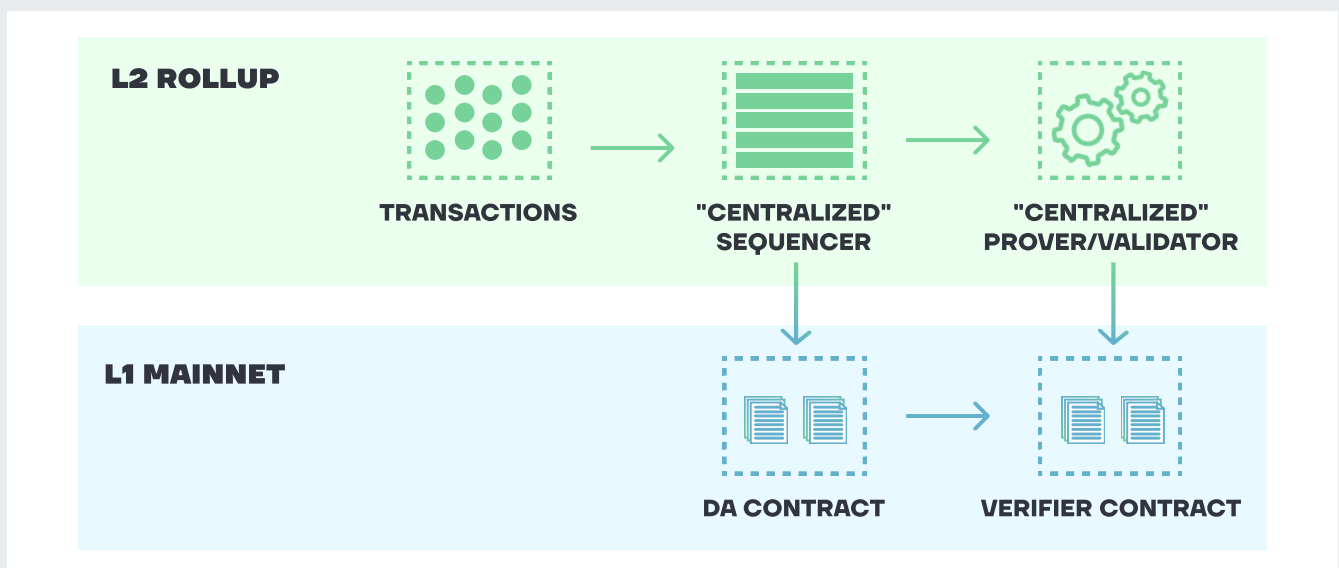


Figure 83. "Centralized" Sequencer and Validator scheme.

Source: Jon Charbonneau: "Rollups Aren't Real".

### Some issues

- ZK-rollups use a supernode - a single operator - as their Sequencer. This centralized structure occasionally results in censorship, and can directly affect the order of transactions.
- Centralized Sequencer may pose challenges in managing the computational processing and proof generation needed to maintain a system's continuous operation. Downtime resulting from various

factors, such as hardware failures, excessive spam, or operational issues, can weaken the uptime of L2 Rollup solutions.

- Moreover, Sequencers have vulnerabilities that expose users to potential financial attacks such as Miner Extractable Value (MEV), including front-running or sandwich attacks.
- Users often encounter significant delays when awaiting confirmation of their transactions in Layer 1, which can adversely affect their overall experience.

## Some Solutions

To address the challenges and enhance user protection in the context of Sequencers, several concept features are being explored:

- **Censorship Resistance Rules:** Users should have the ability to challenge censorship by either forcing a withdrawal from the Rollup or compelling the inclusion of their transactions in L2. This means that L2 users retain the ability to directly include their L2 transactions into the Layer 1 contract, even if they face censorship. Some Rollups are already working on consensus upgrades that incorporate concepts such as inclusion lists, threshold encryption, and additional L2 escape solutions.
- **Economic Instant Finality:** Rather than facing extended confirmation times on Layer 1, users can ensure that Sequencers process their transactions, committing them to a specified index, even prior to L1 confirmation.. If Sequencers failed this commitment, users can detect the breach and submit a claim, potentially resulting in the slashing of the non-compliant Sequencers. Smart contracts equipped with storage proofs can verify these claims.
- **Protection from MEV:** Transaction encryption is employed to safeguard against manipulation by centralized Sequencers. Whilst transactions remain encrypted, the commitment to execute them at a specific index is conveyed to users. This is achieved using a delay mechanism, often in the form of a time-lock puzzle, ensuring protection against MEV-related concerns.

Most Rollups employ a single permissioned Sequencer to submit batches, which can be efficient, but also offer weaker real-time liveness and censorship resistance. Proper safeguards may make this arrangement suitable for many use cases, with the possibility of reserve Sequencers elected by the Rollup's governance. This ensures safety, censorship resistance, and liveness for users. Even in the longer run, a setup with a single active Sequencer could be a viable option. However, considerations around decentralization and censorship still persist, akin to private centralized blockchains.

The implementation of a small Sequencer set or decentralized Sequencers is often viewed as an 'optional' feature for many ZKRs. This expansion of the design space represents a significant improvement over centralized, or custodial solutions, and is not meant to replace maximally decentralized ones. Other aspects, such as user safety, censorship resistance, and reduced trust in Rollup operators, have shown to take precedence.

Four primary Sequencer configurations are being explored, each with its own trade-offs:

- **Centralized Sequencer:** Offers ease of implementation but with suboptimal guarantees on pre-confirmations, liveness, and forced exits.
- **Decentralized L2 Sequencer:** Utilizes a distributed set with meaningful stake, potentially enhancing the robustness of the Rollup. However, this may compromise on factors like latency.



- **L1-Sequenced:** Provides maximum decentralization, censorship resistance, and liveness, but may lack certain features, such as fast pre-confirmations and data throughput limits.
- **Shared Sequencer:** Combines the functionality of a decentralized Sequencer with the benefits of sharing it with others, eliminating the need to create a Sequencer set from scratch. However, it may offer weaker assurances in the interim period before total L1 finality, and can aggregate committee and economic security across many Rollups into one place.

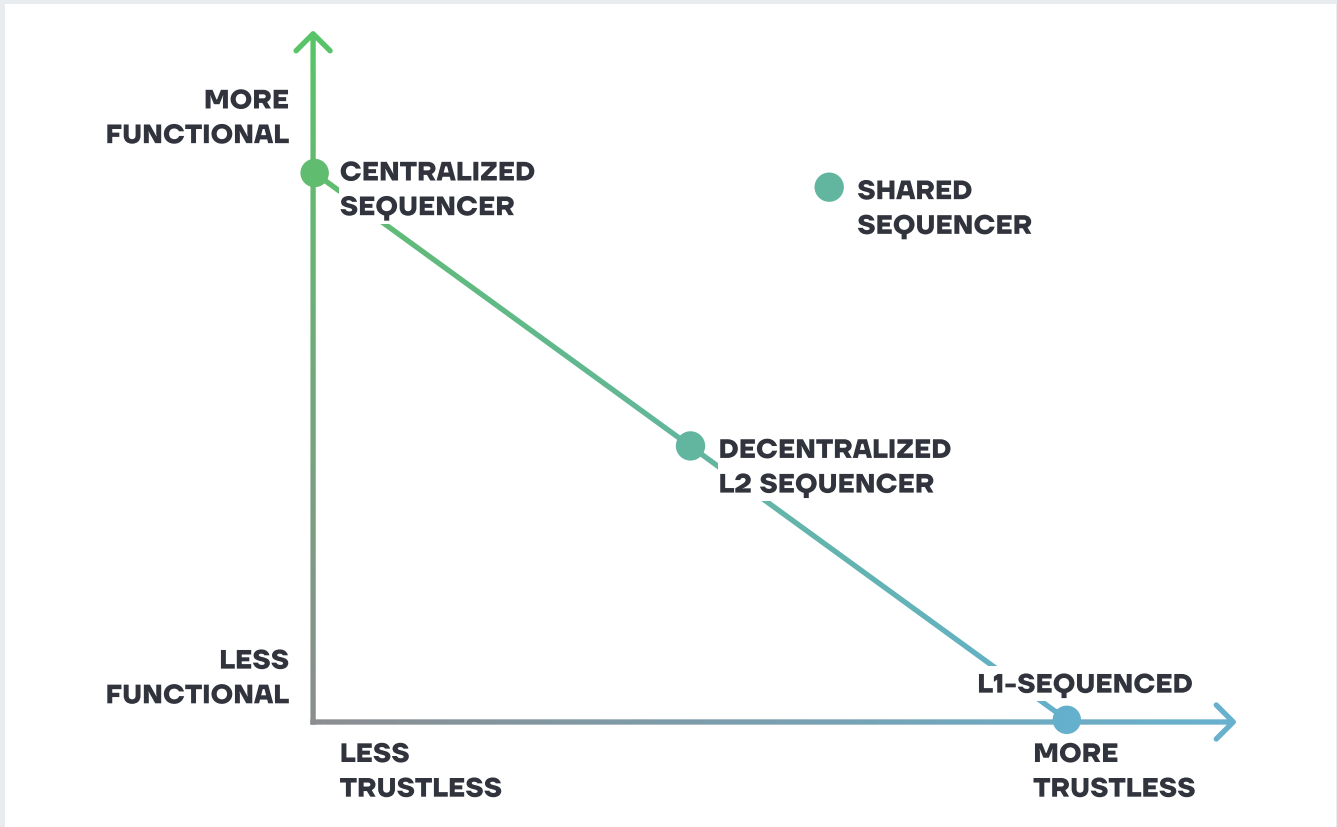


Figure 84. Various Sequencer Designs.  
 Source: Jon Charbonneau: "Rollups Aren't Real".

Efforts to address these challenges involve considering shared, outsourced, or Sequencer solutions, although there are associated trade-offs to be evaluated. It's important to note that it's currently too early to effectively implement these alternatives. Additionally, various concepts related to decentralized Sequencers, including Proof of Authority (PoA), Proof of Stake (PoS) leader selection, Sequencer/Miner Extractable Value (MEV) auctions, and Proof of Execution (PoE), are still in the initial stages of design and development.



**Leona Hioki**  
 Co-founder



INTMAX develops innovations in ZK implementation, making it a unique layer-2 rollup network that offers low cost, security, privacy, and scalability.

We are pioneering a stateless Layer2 rollup network that revolutionizes the Ethereum ecosystem. The INTMAX stateless Layer2 can simultaneously scalability and privacy, which have traditionally been considered difficult to achieve together. With our stateless architecture, validators don't need to maintain extensive databases, allowing for infinite scalability and near-zero gas costs. By introducing an online communication protocol to zkRollup, we eliminate the data availability cost on Layer 1, making transactions more efficient and cost-effective. Our walletless wallet, leveraging biometric authentication and MPC technology, exemplifies our commitment to user-friendly and secure blockchain interactions.



## A DECENTRALIZED INTERLAYER FOR ROLLUPS

### Introduction

AltLayer is innovating in the blockchain space by providing a decentralized interlayer known as the Beacon Layer that connects various rollups to their primary settlement layer. This layer serves multiple functions including sequencing, execution, and verification for rollups created through AltLayer.

### A Decentralized Interlayer for Rollups

Provides decentralized sequencing, rollup state verification, upgrades, etc.

Comes with rollup stack built atop provide SDK and no-code frameworks

A common network between rollups and their DA/Settlement layer to which all rollups are enshrined

### Core Features

In addition to its core protocol, AltLayer offers a user-friendly Rollups-as-a-Service (RaaS) platform. This platform empowers both developers and non-technical users to easily create custom rollups in under two minutes through a simple interface. It supports a range of environments, such as Ethereum Virtual Machine (EVM) and WebAssembly (WASM), and is compatible with multiple rollup SDKs including OP Stack, Arbitrum Orbit, and Starkware.

One of the innovative concepts introduced by AltLayer is the ephemeral rollup. These are temporary rollups that can be rapidly deployed in response to increased demand for an application, used as needed, and then retired with a final settlement on the Layer 1 blockchain. This offers a resource-efficient solution that combines the advantages of both application-specific rollups and general-purpose Layer 1 blockchains.

AltLayer's protocol is designed to reduce both capital and development time, fostering an environment conducive to rapid experimentation and innovation in a permissionless setting. Unlike closed RaaS solutions that are fully managed and lack transparency for the end-users, AltLayer provides a more open protocol that ensures decentralization and allows users to leverage a wider ecosystem, including validators.

## Versatile Rollup Stack

### Sequencer



### Rollup SDKs



### Data Availability



### Interoperability



### Settlement

(Fraud/ZK Proof)



### Data Indexer



### Rollup Type

- Persistent
- On-demand
- Flash Layer
- Ephemeral

### Gas Model

- Priority Gas (1559)
- Gas: L1 Native / ERC20
- FIFO
- Zero Gas / Gas Free

### Proof System

- One-Step Proof
- Bisection Fraud Proof
- Fraud + ZK Proof
- ZK Proof

### Staking / Slashing

- Sequencer
- L2 Token
- Verifier
- Restaking

### Security Guarantee

- Tier 1: Multi Sequencer
- Tier 2: Beacon Layer
- Tier 3: L1 Settlement
- Forkless Upgrade

## ZK Fault Proofs: A new Innovation in the Fault Proof Landscape

The most distinctive research development from AltLayer is the introduction of ZK Fault Proofs, aiming to blend the security benefits of ZK rollups with the operational model of optimistic rollups. This hybrid approach means that cryptographic proofs of correctness are only generated in response to challenges, which could offer significant gas savings and efficiency gains.

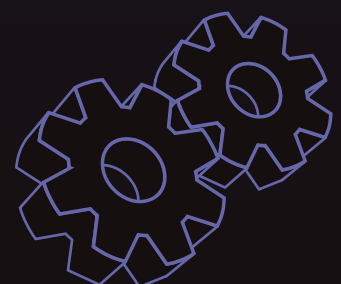
### Implementation by AltLayer using RISC Zero

AltLayer, in partnership with RISC Zero, is developing this concept in two forms: The first variant involves generating a ZK proof for a single contested instruction during a dispute, maintaining most of the existing bisection protocol but adding cryptographic verification. The second variant is more radical, replacing the bisection protocol entirely with a full ZK validity proof, which could substantially decrease the time required for withdrawals from seven days to mere hours or minutes.

Both variants are built on RISC Zero's zkVM, which provides a proving system capable of parallelizable proof generation and supports general-purpose languages, making it suitable for the next generation of rollups. However, these new approaches still depend on the presence of at least one honest participant to identify and challenge any incorrect states.

### Conclusion

AltLayer's ongoing work includes implementing these innovations within major rollup SDKs, providing developers with advanced options for rollup deployment. By doing so, AltLayer is not only streamlining the rollup creation process but also contributing to the overall scalability and security of blockchain infrastructure.



## CONCLUSIONS

- 1. Account Abstraction (AA) in Rollup Architecture:** AA has emerged as a crucial and prominent solution in the realm of Rollup architecture. Given the customizable nature of Rollups (and the fact that some may not support EOAs), AA has become a popular trend in recent years. It has played a pivotal role in enhancing the functionality and security of L2 wallets, setting them apart from traditional services. Even the fundamental features of Account Abstraction offer significantly more capabilities compared to regular EOAs. Positive user experience is a primary driver for adoption, and continuous improvements in AA tools are enhancing the ecosystem for both ordinary users and developers. By incorporating various management, development, and security SDKs, it is possible to create a high-quality portal that offers a constructive experience within the rollup ecosystem. Remarkably, influential financial institutions like Visa are considering Account Abstraction-based L2 solutions as the most optimal choice for their operations.
- 2. Developments in 2023 for zkEVM, zkVM, Compilers, and SDKs:** In 2023, there has been notable advancement in the development of zkEVM and zkVM, as well as the creation of Compilers, SDKs, and other tools tailored for developers. With a 22% decline in the number of Web3 developers since their peak in 2022, there is an increasing demand for developers to acquire new programming languages to build dApps on ZKR. Some developers are addressing this challenge by abstracting code, using compilers, or modifying it to resemble more familiar programming languages such as Solidity, Rust, Go, Typescript, among others. Efforts are underway to develop educational resources and improve the code base to expand the potential functionality of dApps on ZKR. Furthermore, active grant programs are being introduced to incentivize participation in new L1 and L2 blockchains, thereby promoting growth and innovation in the sector.
- 3. Diverse Approaches in the ZKR Space:** It is fascinating to observe the varied approaches taken by different teams in the ZKR space, as they make strategic decisions based on contrasting anticipated outcomes. Some teams have either achieved, or are close to reaching the Ethereum equivalent of zkEVM, and are proactively onboarding projects from Layer 1 to expedite the growth of their unique ecosystem. These projects rely on the privacy and high performance of their code to surpass the achievements of the EVM. In contrast, some opt for a more universal approach, working bidirectionally to maintain options. Such diversity indicates a healthy market segment where every entity is simultaneously a competitor and potential partner, fostering innovation and competition.
- 4. Hyper-Scaling and Interconnected Blockchain Ecosystems:** In 2023, the blockchain domain has witnessed a significant shift towards hyper-scaling and the development of Layer 2 to Layer 3 solutions. This shift is underscored by the launch of essential tools and frameworks such as ZK Stack, StarkEx, Kakarot zkEVM, and Polygon CDK. These innovations have facilitated the creation of modular and interconnected structures, enabling seamless communication between L1 and L2, L2 and L2, as well as L2 and L3. Among these advancements, zkEVM Taiko has been instrumental, offering an open-source framework for crafting ZK-based Layer 2 blockchains. It has gained significant traction, especially through platforms like Polygon CDK. Such advancements fuel the growth of varied ecosystems, heighten competition, and enable the deployment of highly specialized components, fostering a dynamic and interconnected blockchain landscape.

Moreover, the emergence of modular solutions such as Celestia and EigenLayer, albeit in their early stages, holds potential to complement the architecture of rollups and address specific requirements.

Looking ahead, further enhancements in Validiums, Data Availability Committees schemes (DACs), Bridges, and zkOracles are expected to enhance system reliability and efficiency. This sets the stage for a surge in new cross-rollup and L1 to L2 infrastructure solutions in 2024, offering promising advancements in the scalability, security, and usability of blockchain technology for the upcoming year.

**5. Advancements in ZKP Technology in 2023-2024:** 2023 marked considerable research and developments in the field of Zero-Knowledge Proof (ZKP) schemes. Notable milestones included the introduction of zk-STARK Bujoom shadow validation by zkSync, the launch of Plonky3, and Polygon's shift to zkEVM. These advancements highlight the ongoing evolution and optimization of ZKP technology. However, despite these advancements, there remains a need to empirically validate these theoretical concepts, especially regarding the security and quantum stability of rollups. Comprehensive testing is crucial to ensure the robustness and reliability of these solutions in real-world scenarios. Additionally, numerous research findings underscore the crucial role that the privacy component plays for users.

The efficacy of ZKPs cryptography cannot be evaluated in isolation. It is imperative to analyze the current infrastructure for creating ZK-proofs, the effectiveness of logical schemes, and pivotal roles played by Sequencers, Validators, and Layer 1 smart contracts. Key priorities for ZK-building teams include achieving consensus, addressing risks tied to cryptographic protocols, minimizing ecosystem maintenance costs, and enhancing hardware components. The intricate challenges within this domain have led to the emergence of specialized service providers offering focused tools such as ZKP Hardware programming and the outsourcing of Sequencer Layers. It remains to be seen how ZK Rollups will tackle these challenges ahead of a potential full-scale launch of hyper-scalable and privacy-oriented infrastructures.

**6. Growing Interest and Activity:** The past year has witnessed a significant surge in interest within the crypto community and representatives of the Web2 industry. Notably, the market has remained active throughout bear cycles, evident from consistent commits and regular developer engagement. The rising popularity of Web3 development in various regions, including America, Europe, and the East, is reflected in the increasing number of events and hackathons. Acceleration budgets in various ecosystems, especially those focused on ZKR-based dApps, are providing an impetus for new ideas, potentially leading to a resurgence in development activity with an improvement in market conditions. With the burgeoning number of ecosystems offering better tools, guides, schools, and DAOs, the direction of Web3 development is just beginning to unfold on a large scale. Blockchain developers, equipped with knowledge of classical programming languages, are expected to remain in high demand in the upcoming years.

**7. Optimization of ZKP Hardware:** The field of optimizing ZKP Hardware to enhance the generation of zk-SNARKS and zk-STARKS represents a significant area for innovation. The price and efficiency of computing and hardware solutions directly impact user experiences and the value they offer. The diverse range of cryptographic schemes and hardware configurations presents opportunities for creating new and more efficient solutions, which are currently in their initial phases of implementation. The upcoming year may witness groundbreaking advancements in these areas, potentially leading to a revitalization of the mining industry to support Layer 2 solutions. Emphasis on the logical architecture is equally important, with each ecosystem separately developing more efficient models for Sequencers, Validators, and L1 smart contract management. While L2 solutions may not achieve the same degree of decentralization as L1 Ethereum in the foreseeable future, the crypto community is likely to continue embracing them because of the trade-offs they present.

# 6 ABOUT THE AUTHORS

## ABOUT THE AUTHORS



**Vadim Krekotin**  
Founding Partner



**Alex Mukhin**  
Managing Partner



**Ivan Semenov**  
Managing Partner



**Grigoriy Murrban**  
Associate



**Nikita Smohorzhevskiy**  
Analyst



**Daniyar Sakhibuddin**  
Research intern

## ABOUT CRYPTOMERIA CAPITAL

Cryptomeria Capital is an early-stage VC firm based in Dubai with presence in Singapore and HongKong. The firm believes decentralized projects, cryptocurrencies, and Web 3.0 will dramatically reshape economic relations and focuses on ventures, tokens, and projects related to blockchain technology and crypto assets. Cryptomeria Capital supports transformation by providing early-stage financing for ambitious projects in a rapidly developing industry.

## ABOUT AXON PARTNERS, BME:APG

With international presence and global reach, Axon has 2 different business units: alternative investment and strategic consulting that offer their services in more than 70 countries, with high exposure to the Americas, Europe, Middle East and Southeast Asia.

**2006**

Year founded

**>50**

Companies backed

**12**

Funds

**+100**

Years of accumulated  
experience of the partners

**+85**

Employees

# BIBLIOGRAPHY

1. "Starknet Documentation".
2. "Starknet Book".
3. "StarkEx Documentation".
4. "zkSync User Documentation".
5. "Era zkSync Documentation".
6. "Scroll Documentation".
7. "zkEVM on Polygon Wiki".
8. "Aztec Network Documentation".
9. "Aztec Network Developer Documentation".
10. "Taiko Documentation".
11. "Linea Documentation".
12. "Loopring Documentation".
13. "Kroma Network Introduction".
14. "Mina Protocol Documentation".
15. "Manta Network Documentation".
16. "Aleo Developer Documentation".
17. Vitalik Buterin: "zkEVM: The Road Ahead", Blog, August 4, 2022.
18. Vitalik Buterin: "An Incomplete Guide to Rollups", Blog, January 5, 2021.
19. ZKValidator: "The State of ZK Q2 2023", Report, July 17, 2023.
20. L2Fees.info.
21. L2Beat.com.
22. ScalingX Research: "Sequencer for L2 Solutions", Medium, September 26, 2023.
23. Jon Charbonneau: "Rollups Aren't Real", Substack, March 19, 2023.
24. Ben Kiepuszewski (Tweet): Sequencer and Validator, Twitter, February 9, 2023.
25. msfew: "AI Rollup with AI oracle proof", Mirror, April 16, 2023.
26. msfew: "Risks of Rollup", Mirror, May 10, 2023.
27. Vishal Chawla: "A16Z Crypto: Zero-Knowledge Proofs", The Block, August 10, 2023.
28. Amber Group: "The Need for Speed: Zero Knowledge", Medium, September 5, 2022.
29. Figment Capital: "Accelerating Zero-Knowledge Proofs", Medium, April 25, 2023.

## BIBLIOGRAPHY

30. OxMonia: "Hardware Review", HackMD, September 2023.
31. Byron from Loopring: "Loopring + Taiko: Ready Layer 3", Medium, June 7, 2023.
32. Margaux Nijkerk: "Scroll zkEVM Launches", CoinDesk, October 12, 2023.
33. Justin Thaler: "Snark Security and Performance", A16Z Crypto, December 9, 2022.
34. Infura: "Solving Blockchain Scalability with DAC", Blog, October 13, 2022.
35. zkValidator: "A Survey of zk Languages", Blog.
36. Juan Leal from Thirdweb: "Which zkEVM is Best?", Blog, August 9, 2023.
37. Jarrod Watts: "The Ultimate zkEVM Comparison Guide", Blog, July 15, 2023.
38. Aayush Gupta: "ZK Tooling and Proof Systems", Blog, September 1, 2023.
39. Daniel Wang: "A Concise Dive Into Taiko ZK-Rollup", YouTube, September 15, 2023.
40. Matter Labs: "zkPorter: A Breakthrough in L2 Scaling", Medium, April 13, 2021.
41. Matter Labs: "Introducing the zk-Stack", Medium, June 26, 2023.
42. zkValidator: "zkEVMs Beyond Polygon and zkSync", Blog.
43. Ye Zhang: "zkEVM circuit arithmetization", YouTube, April 21 2022.
44. Starkware: "Volition and the Emerging Data Availability", Medium, June 14, 2020.
45. StarkWare: "Fractal Scaling: From L2 to L3", Medium, December 21, 2021.
46. Taiko Labs: "Taiko Protocol Overview", Mirror, May 2, 2023.
47. Taiko Labs: "Taiko Roadmap", Mirror, March 9, 2023.
48. Ezkl: "zkonduit" Github, August 2023.
49. Ethereum Foundation: "Zero Knowledge Machine Learning", Youtube, November 15, 2022.
50. AleoHQ: "Aleo Curves", Medium, February 25, 2023.
51. Loopring Protocol: "Loopring Quarterly Update Q2 2023", Medium, April 15, 2023.
52. Manta Network: "A Scalable, Secure, and Private Layer 2 for Ethereum, Manta Network", Medium, June 20, 2022.
53. Rootz Labs: "Why Scroll is Different from All ZKRollups, Rootz Labs", Medium, August 2, 2022.
54. Coindesk: "Ethereum zkEVM: Scroll Network's Scalability Play", Medium, September 15, 2023.
55. Medium: Scroll zkEVM: "The Leader Among Others", Medium, July 13, 2023 .
56. Covalent:" zkEVMs, Covalent", Medium, July 25, 2023.
57. Scroll: "Kzg: A New Approach to Zero-Knowledge Proofs, Scroll", Blog, August 27, 2023.
58. Scroll: "Proof Generation, Scroll, Blog", September 22, 2023.



## BIBLIOGRAPHY

59. Dune: “Kroma ZK-EVM Layer 2, Dune”, Medium, October 2 2023.
60. Kroma Network: “The Road to Kroma's Decentralization”, Medium, October 22, 2023.
61. Kroma Network: “An overview of Kroma's architecture”, Blog, November 15, 2023.
62. Kroma Network: “Introduction to Kroma”, Medium, November 29, 2023 .
63. Coindar: “Loopring (LRC), Coindar”, Medium, January 10, 2023.
64. Loopring Protocol: “Loopring Quarterly Update Q1 2023”, Medium, January 30 2023.
65. Loopring Protocol: “Counterfactual wallet NFTs on Loopring”, Medium, February 20, 2023.
66. Loopring Protocol: “L2 DeFi port, Loopring Protocol”, Medium, March 10 2023.
67. Linea: “Apps, Linea, Website”, March 30, 2023.
68. Linea: “Linea: A scalable, secure, and private Layer 2 for Ethereum, Linea, Mirror”, April 20, 2023.
69. Thirdweb: “Polygon zkEVM vs ZKSync Era vs Linea vs Scroll vs Taiko, Thirdweb, Blog”, May 10, 2023.
70. Aztec Protocol: “An introduction to Aztec”, Medium, May 30, 2023.
71. o1-labs: “A JavaScript library for building secure and private applications”, GitHub, June 20, 2023.
72. Haresh Gedia: “Mina Protocol: Nil Foundation - A bridge to Ethereum, Haresh Gedia, Medium”, July 10 2023.
73. Aztec Protocol: “Aztec's private smart contract framework”, Medium, July 30, 2023.
74. Aztec Protocol: “Zero-knowledge gaming with BattleZips x Noir”, Medium, August, 20 2023.
75. Aztec Labs: “Aztec grants round 2, Aztec Labs”, Medium, November 1, 2023.
76. Aztec: “The Hybrid zkRollup”, Aztec Labs, Blog, May 4, 2022.
77. Electric Capital: “October 2023 Developer Update”, Blog, October 18, 2023.
78. zkRollups: “What id Loopring?”, Blog, August 14 2022.
79. Binance News: “How ZK Proof Startup Cysic Breakthrough in the ZK Hardware Acceleration Roadmap”, Binance, February 22, 2023.
80. Keep StarkNet Strange: “Garaga”, Github, October 2, 2023.



**CRYPTOMERIA  
CAPITAL**

**Disclaimer:**

This article is based on open publicly available sources and, while we have made every effort, we cannot guarantee accuracy or reliability of the information provided.

Furthermore, this article should not be interpreted as investment or financial advice, and readers should always do their own research or consult with professional consultants before making any decisions related to their finances.

**FOR FURTHER CONTACT**

If you would like to discuss this report, share ideas or say 'Hi', please contact [contact@cryptomeriacapital.com](mailto:contact@cryptomeriacapital.com)

[cryptomeriacapital.com](http://cryptomeriacapital.com)



[@CryptomeriaCap](https://twitter.com/CryptomeriaCap)