



**CRYPTOMERIA  
CAPITAL**

In corporate partnership with AXON 

# ZK-ROLLUPS LANDSCAPE OVERVIEW

**July 2023**

# DEAR PARTNERS, INVESTORS, AND FRIENDS

“

We are excited to share with you this in-depth analysis of ZK-rollups. In this report, we have gathered all the essential information about ZK-rollups, an important solution and highly anticipated trend of the upcoming bull market.

By addressing scalability challenges in the blockchain networks, ZK-rollups will enable private and secure off-chain transaction aggregation, reducing transaction fees, and improving transaction throughput. As demand for Ethereum scaling solutions continues to increase, ZK-rollups could become one of the strongest-performing sectors in 2023. This element of blockchain technologies will significantly change the overall crypto ecosystem, and will play a major role in the future of Web3, decentralized finance and the metaverse.

We are proud to discover the great potential of ZK-rollups at an early stage of their development, staying ahead of the trends. We hope this report will provide you with the much-needed information on these new tools and become an indispensable guide to all the details of ZK-rollup technology

”



**VADIM KREKOTIN**

Founding Partner at  
Cryptomeria Capital





# RESEARCH PARTNERS

**HASHKEY**  
Capital

 **polygon zkEVM**

 **Scroll**

**ZKX**

 **INTMAX**

 **ZKEX**

 **Hashstack**

 **ZKPASS**

 **Veridise.**



 **Rádus**

**ANTALPHA  
VENTURES**

 **SCALINGX**

 **SPACE SHARD**


 **PRAGMA**

# COMMUNITY PARTNERS

 **STARKNETICS**  
All Starknet Ecosystem in your pocket

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

 **zkSync Rater**  
Zero-knowledge might be easy  
with us, stay updated with the  
latest news & insights here!

 [@zksync\\_ing](https://twitter.com/zksync_ing)

**ZK SEASONS**  
Community Events Worldwide

**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

1. Key takeaways .....	5
2. What are rollups, and why are they needed? .....	6
3. Bulletproofs .....	8
4. Rollups .....	9
5. Zero-knowledge and optimistic rollups .....	11
6. ZK-SNARK and ZK-STARK proofs .....	17
7. ZK-rollup ecosystem .....	24
I. zkSync .....	24
II. StarkNet .....	29
III. Scroll .....	36
IV. Intmax .....	40
V. Aztec Network .....	41
VI. Polygon .....	44
8. About the Authors .....	53
9. Bibliography .....	54





# KEY TAKEAWAYS

- The concept of zero-knowledge rollups (ZK-rollups or simply ZKR) was originally created back in 1989. Since then, a number of different solutions have been created: optimistic rollups and ZK-rollups, as well as other technologies like Bulletproofs.
- Optimistic rollups offer a significant advantage in terms of lower costs compared to ZK-rollups. This cost reduction is primarily due to the absence of proof requirements for transactions unless they are specifically challenged. On the other hand, Zero-knowledge rollups tend to incur higher network costs due to the computational proof needed for every transaction block, as well as the necessity for powerful hardware to carry out these computations. By leveraging the optimistic approach, optimistic rollups achieve cost efficiency and scalability, making them a compelling choice for certain use cases.
- However, there is an important consideration for optimistic rollup (OR) users that may result in a waiting period for L2 to L1 withdrawals. This waiting period, typically around seven days, is necessary to ensure the safety of the chain and to allow for any potential disputes to be resolved using fraud proofs. On the other hand, Zero-knowledge rollup users do not face such delays because all transactions come with validity proofs, enabling immediate changes to the network state without any concerns of fraud. This distinction allows ZKR users to enjoy faster and more seamless transactions, eliminating the need for waiting periods.
- Previously, ZK-STARK differed from ZK-SNARK in quantum stability and did not require trusted installations. However, recent implementations of ZK-SNARK have quantum stability, do not require trusted setups, and have a smaller proof size than ZK-STARK. What's more, ZK-SNARK currently offers a much lower transaction cost than ZK-STARK.
- Optimistic rollups offer EVM compatibility, simplifying development and allowing easy integration of Ethereum apps. In contrast, ZK-rollups lack full EVM compatibility, requiring code adaptation and specialized knowledge. However, some ZK-rollups are working on code compilers and validity proof converters to improve their EVM compatibility and attract more developers and new ecosystem projects.



# WHAT ARE ROLLUPS, AND WHY ARE THEY NEEDED?

The history of ZK-rollups begins in 1989 with the publication of "The Knowledge Complexity of Interactive Proof Systems" by MIT researchers Shafi Goldwasser, Silvio Micali and Charles Rackoff. The paper introduced the idea of zero-knowledge proofs and presented key concepts, including the interactive proof hierarchy. It proposed the concept of knowledge complexity, which measures the amount of information the proving agent must know in order to convince the verifier of the validity of a claim. The researchers gave the first proof with zero knowledge for a particular problem, which was a significant achievement.

And in 1993, researchers from the University of Chicago and the University of Budapest published "Arthur-Merlin Games: A Randomized Proof System and a Hierarchy of Complexity Classes". The article introduced the concept of randomized proofs that combine zero-knowledge and traditional proof theory.

In 2017, more than two decades later, it became clear that Ethereum was no longer capable of covering user requests for fast and cheap transactions on its own. An example is the DeFi Boom and Bull runs in 2017 and 2021 when limited bandwidth led to huge gas costs of hundreds of dollars. Therefore, the main tasks of Ethereum are:

- Minimize transaction fees;
- Improve network capacity and scalability;
- Reduce potential blockchain space load.

All led to the search for ways to scale Ethereum, the first option of which was Plasma. Along with the rising popularity of Ethereum came the awareness that the blockchain needed scaling solutions. The result was the Bulletproofs technology from Stanford's Applied Cryptography Group and Plasma, presented by Joseph Poon and Vitalik Buterin at a meetup in San Francisco.

Plasma was designed as an Ethereum sidechain with minimum trust in sidechain operators. It prevents funds from being stolen even if operators (or a consensus majority) didn't publish the underlying transaction data.

While the Plasma MVP was not ultimately adopted, it laid the groundwork for future development of optimistic rollups. However, the Plasma MVP launch highlighted several inconveniences and architectural flaws. Users were burdened with the need to constantly monitor the validity of transactions within the network to prevent fraudulent batches and avoid being caught in the challenge period. Withdrawals were subject to delays of up to one week, and anyone could initiate additional validations. Furthermore, in the event of mass exits, there was a concern that Ethereum could become overloaded, exacerbating the challenges during a period of high network activity like a bull run. These issues underscored the need for further scalability and security improvements within the context of optimistic rollups.

In 2018, an anonymous GitHub user with the pseudonym Barry Whitehat published a repository [roll\\_up](#), a new idea for layer-2 scaling with SNARK proofs that did not require users to trust anyone. Soon after, Buterin released an improved version of Barry's proof called zero-knowledge rollups.





These two developments breathed new life into developing L2 solutions for Ethereum by mid-2019, boosting zkSync, Starkware, and others. But for all their advantages, zk-rollups had one major disadvantage: Ethereum smart contracts cannot be deployed directly on them. You need separate virtual machines or development tools to use smart contracts.

Optimistic rollups offer a significant advantage in terms of lower costs compared to zero-knowledge rollups. This cost reduction is primarily due to the absence of proof requirements for transactions unless they are specifically challenged. However, zero-knowledge rollups tend to incur higher network costs due to the computational proof needed for every transaction block, as well as the necessity for powerful hardware to carry out these computations. By leveraging the optimistic approach, optimistic rollups achieve cost efficiency and scalability, making them a compelling choice for certain use cases.

However, there is an important consideration for optimistic rollup (OR) users that may result in a waiting period for L2 to L1 withdrawals. This waiting period, typically around seven days, is necessary to ensure the safety of the chain and to allow for any potential disputes to be resolved using fraud proofs. On the other hand, ZK-rollup users do not face such delays because all transactions come with validity proofs, enabling immediate changes to the network state without any concerns of fraud. This distinction allows ZK-rollup users to enjoy faster and more seamless transactions, eliminating the need for waiting periods.

“



**ANDY GUZMAN**

Product Owner at  
Privacy Scaling  
Explorations, part of



One of the most exciting areas for zero knowledge is the intersection with account abstraction and layer2s to improve the user experience on Ethereum. ZK can leverage external digital signatures that exist in mainstream applications and bring existing web2 flows to web3.

This means that familiar authentication methods like FaceID, TouchID, WebAuth, to mention a few, can be seamlessly integrated into Ethereum transactions, allowing users to authenticate their actions while preserving the decentralized and censorship-resistant nature of the blockchain. This also means familiar physical and digital identifications like government IDs, passports, and NFC cards that leverage public-key cryptography, can be used as authentication methods to approve transactions.



PrivacyScaling  
explores new use  
cases for zero-  
knowledge proofs and  
other cryptographic  
primitives through  
research and proof-  
of-concepts.

An additional feature of ZK lies in its capacity to aggregate transaction proofs, with the potential to result in low gas costs for users. In fact, this capability has the potential to achieve even lower gas costs than what was previously attainable through alternative methods. By consolidating and combining the proofs that represent transactions, ZK brings forth an efficient and cost-effective solution that ensures users can execute transactions on Ethereum without incurring exorbitant gas fees. This advancement in gas cost optimization further enhances the affordability and accessibility of Ethereum.

The potential for incorporating public-key cryptography-based applications into Ethereum's ecosystem is vast. With ZK-proofs acting as a bridge between different cryptographic systems, Ethereum becomes more adaptable and versatile. Any application that relies on public-key cryptography, from secure messaging systems to identity verification protocols, can seamlessly integrate with Ethereum.

”



# BULLETPROOFS

All Bulletproofs work based on the Pedersen commitment, a cryptographic algorithm that allows the checker to accept a specific value without revealing it to the checker and without allowing him to change it.

The concept of Bulletproofs was proposed in 2017 by the Stanford Applied Cryptography Group, which was responsible specifically for anonymizing transactions. They base on so-called range proofs, which do not provide an exact amount but indicate that the secret is within a given range and is an improvement over range proofs.

Bulletproofs are designed to provide efficient and confidential crypto transactions. Confidential transactions hide the amount that is transferred in a transaction while providing cryptographic proof that the transaction is valid.

Bulletproofs reduce the size of the cryptographic proof from more than 10 KB to less than 1 KB. If all bitcoin transactions were confidential and used Bulletproofs, the total length of the UTXO set would be only 17GB compared to 160GB with the current proofs.

There is one crucial difference between range proofs and Bulletproofs: Range proofs encode the entire range with more transaction info and have fixed block sizes. As range proofs must cover a larger range of data, they can easily overload blockchain memory space. This is a significant disadvantage in the long run.

Bulletproofs is less than 1kb in size. In addition to saving block space, it reduces transaction costs by combining multiple transaction range proofs into a single proof and putting more transactions in a block.

Bulletproofs can also be used for multilateral computation as they can combine multiple proofs of multiple ranges, with multiple parties having access to only their part of the information in the proof. Monero, which previously used range proofs, has switched to this technology. Unlike the first ZK-SNARK implementations, Bulletproofs do not require a trusted setup. Utilizing Bulletproofs for handling smart contracts can be expensive and relatively easier for anonymizing transfers. However, when it comes to cost-effectiveness and resource efficiency, rollup technology takes the lead. As a result, the primary focus of development is directed towards optimistic and zero-Knowledge rollup technologies. These solutions offer more cost-effective and streamlined approaches to scalability, making them the preferred direction for further advancements in the field.



Bulletproofs possess immense potential to revolutionize the usability and security of zero-knowledge proofs, thereby making them more practical and efficient for deployment in a diverse range of applications. The impact of bulletproofs extends to the areas that require privacy, security, transparency, and trustlessness. As research and development in this area continue to progress, bulletproofs are likely to play a significant role in reinforcing the privacy and security of decentralized systems, while also laying the foundation for widespread adoption of ZKPs across diverse real-world use cases.



**IVAN SEMENOV**

Managing Partner at Cryptomeria Capital





# 4 ROLLUPS

Rollups are separate layers that absorb the burden of executing transactions on L2 so L1 Ethereum can focus on consensus and data availability, a perfect solution for the capacity and security of transactions.

Transactions are much cheaper as gas fees are related to execution. If execution is going in off-chain and many transactions are compressed in only one batch on the way to L1, the transaction will be much cheaper than regular Ethereum transactions.

Rollups often perform state storage and off-chain calculations but store some data for each on-chain transaction. They can send a bunch of transactions executed on L2 to L1 in a single transaction, attaching proof of validity.

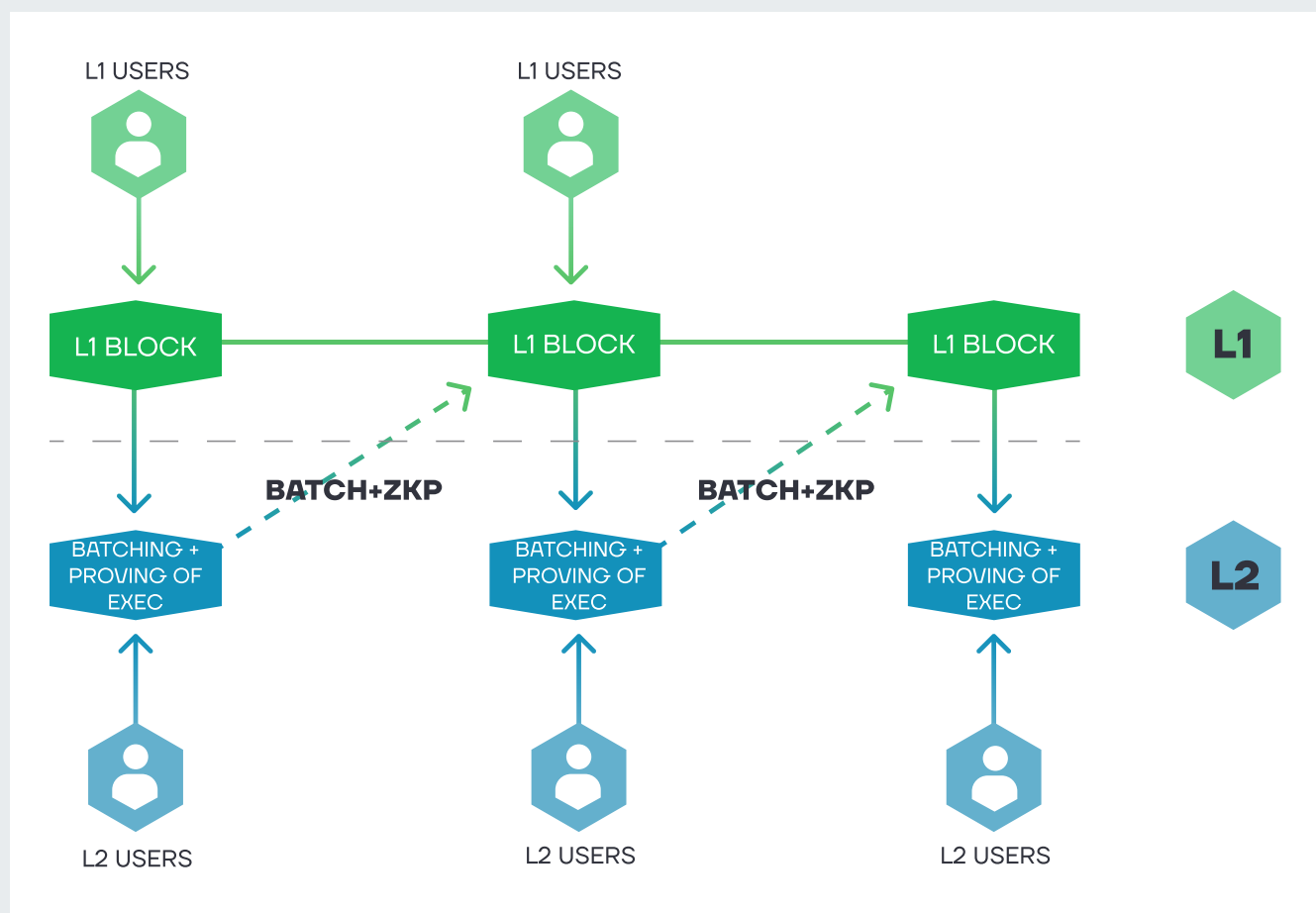


Figure 1: Transaction path between L1 and L2.

Source: *An Overview on ZK-Rollups and zkEVM*

Rather than recording each transaction on the blockchain, a hash is generated to verify their accuracy. This approach significantly saves block space and reduces the cost of each transaction by approximately 150 times compared to the costs on the Ethereum network. By leveraging this solution, the efficiency and affordability of transactions are greatly enhanced, providing substantial benefits in terms of both resource utilization and cost savings.

Hashing is a way of recording data information in a fixed-length string. Any modification to that data drastically changes the hashing to ensure that each incoming data set is valid.

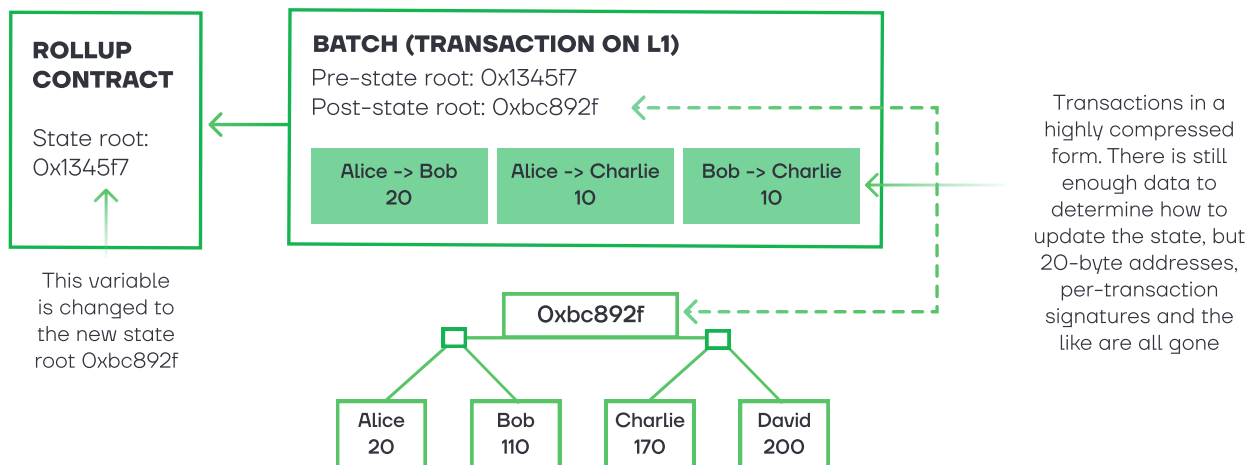


Figure 2: zk-Rollup Architecture

Source: Source code analysis of zkSync, Liozhu

Merkle root of the actual rollup state stores all the critical information on what happens on-chain inside the rollup, including account balance and contract code. When a transaction packet is transmitted in a highly compressed form, the root of the previous state and the root of the updated state are attached to it. The transaction also stores information about new inputs/outputs to/from rollups, allowing for the efficient exchange of L2 and L1 current on-chain information and maintaining transparency for validation. However, transaction verification needs something else – to check proofs about root state and transactions verification. So, nowadays, to solve this problem, we have two main categories – optimistic rollups with fraud proofs and trustless zero-knowledge rollups.

“



**JUPITER ZHENG**

Research Director at  
HashKey Capital

The blockchain industry is currently witnessing an increase in the number of zero-knowledge proof projects, especially the emergence of zero-knowledge proof applications at the level of scaling and privacy protection. Due to the mathematical nature of ZKP, it may be difficult for the average person to understand ZK in depth. Therefore, it is very important to systematically organize all knowledge points of the ZK industry.

A lot has been spoken recently about the development of zkEVM, which is also the focus of the work of the leading projects. Hardware supporting zkEVM proofs will start to appear late this year or early next year. Furthermore, we should note that zkVM also has a relatively large potential: zkBridge may change the verification process on light clients to ZK-proof.

ZK projects' performance after going online is actually a prerequisite for whether they can be applied on a large scale, and it can be assumed that Cancun's upgrade to reduce the cost of layer 2 will make the zk technology-backed layer 2 better adaptable.

**HASHKEY**  
Capital

HashKey Capital is an institutional asset manager investing exclusively in blockchain technology and digital assets and has managed over US\$1 billion in client assets since inception.

As one of the largest crypto funds based in Asia and known for being Ethereum's earliest corporate investor in the region, our mission is to bridge crypto to the mainstream while connecting web2 and web3.

HashKey Capital operates in Hong Kong, Singapore, Japan and the U.S. and has invested in over 200+ projects since 2015.

With profound knowledge of the blockchain ecosystem in the region, the team has built a network connecting entrepreneurs, investors, developers, community participants, and regulators.

Among portfolio:



”



# ZERO-KNOWLEDGE AND OPTIMISTIC ROLLUPS

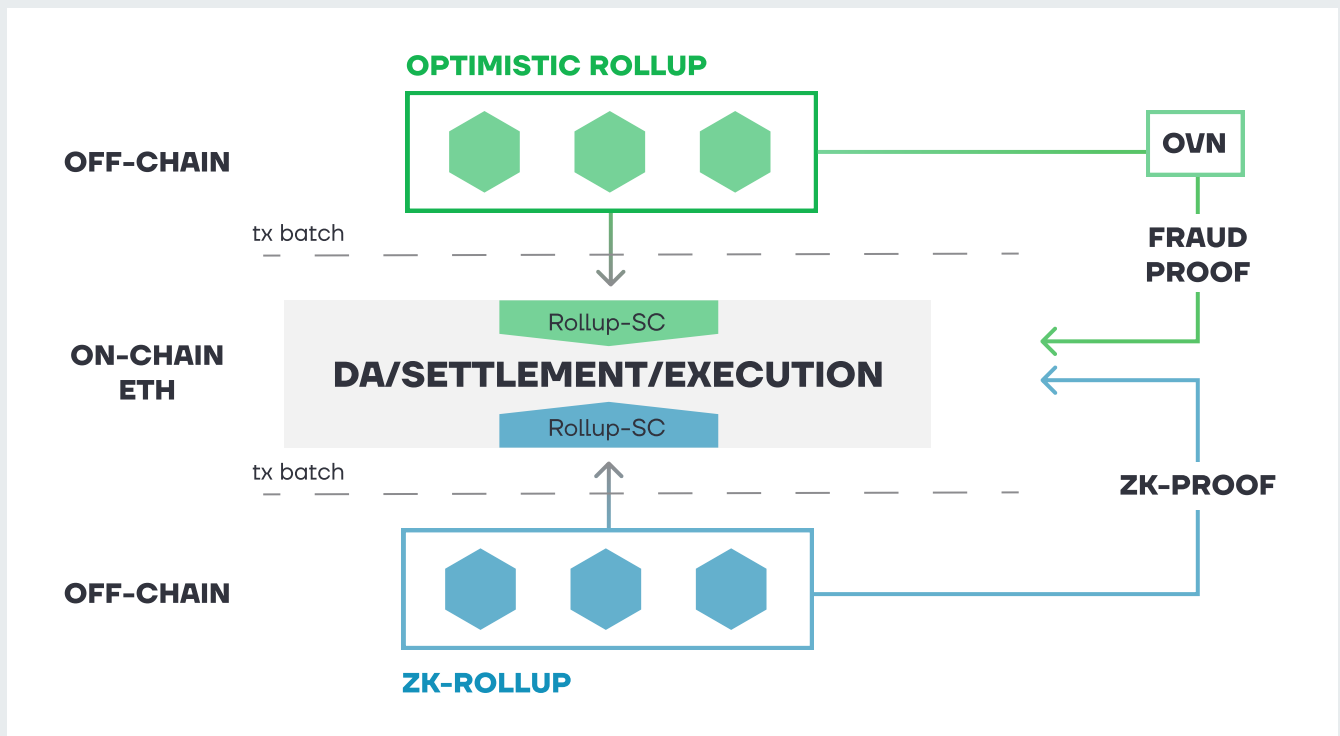


Figure 3: Comparison of the general architecture principles of optimistic rollups and ZK-rollups.

Source: The Modular World, Maven 11 research

The name optimistic rollups (OR) perfectly sums up the logic on which they operate. The default assumption is that all transactions are correct. Fraud Proofs are generated if there is a request to check the fact of fraud or dispute, which is easier to carry out than ZK-proofs, as they must be calculated for every block. Plasma Chain was the first to successfully implement fraud proofs.

Since there is no proof of the correctness of each transaction, after a rollup batch is submitted to Ethereum, there is a delay, usually a seven-day period, when transactions can be challenged. If a challenge occurs during the challenge period, fraud proofs are carried out to ensure no fraud has been committed. The package is considered fraudulent if the calculated root after state and the provided root after state do not match when checking.

The longer the delay, the more chances to detect incorrect data during state transition, but it also means that for those whose transactions are valid suffer. And in theory, even with a challenging period of a week, there could be risks of either passing undetected incorrect charges or a 51% attack when the state the fraudsters want is finalized. In addition, such a limitation significantly reduces capital efficiency.

That's why optimistic rollups and zk-rollups use permissioned-sequencers that process transactions, create rollup blocks, and send transactions to L1 (Ethereum). optimistic rollups use whitelists of validators as a system built on Fraud Proofs requires more trust from validators than other systems.

Some solutions issue funds to users against an outgoing transaction to level out withdrawal delays, acting as liquidity providers. These include the L2 Boba Network and bridges.

Optimistic rollups are compatible with Ethereum from high-level RPC to low-level bytecode because of the lack of complex calculations, making it easy to implement geth.

OR's native compatibility with EVM allows the same dApps from L1 to be ported and deployed to L2 as quickly as possible without any code changes. This central point makes the OR ecosystem grow faster than ZKR.

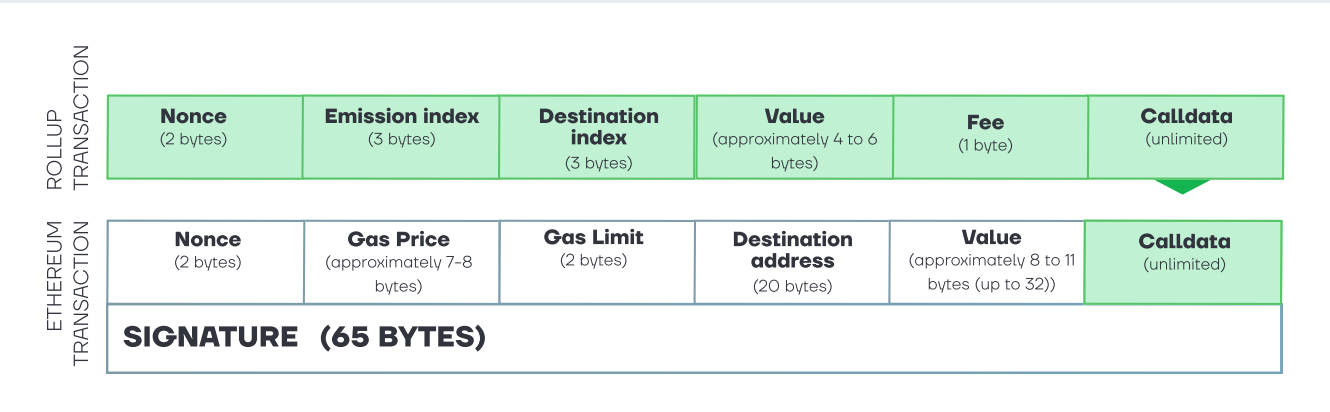


Figure 4: Integration of a rollup transaction into an Ethereum transaction.  
Source: Enabling Blockchain Services for IoE with Zk-Rollups Thomas Lavour, Jérôme Lacan, and Caroline P. C.

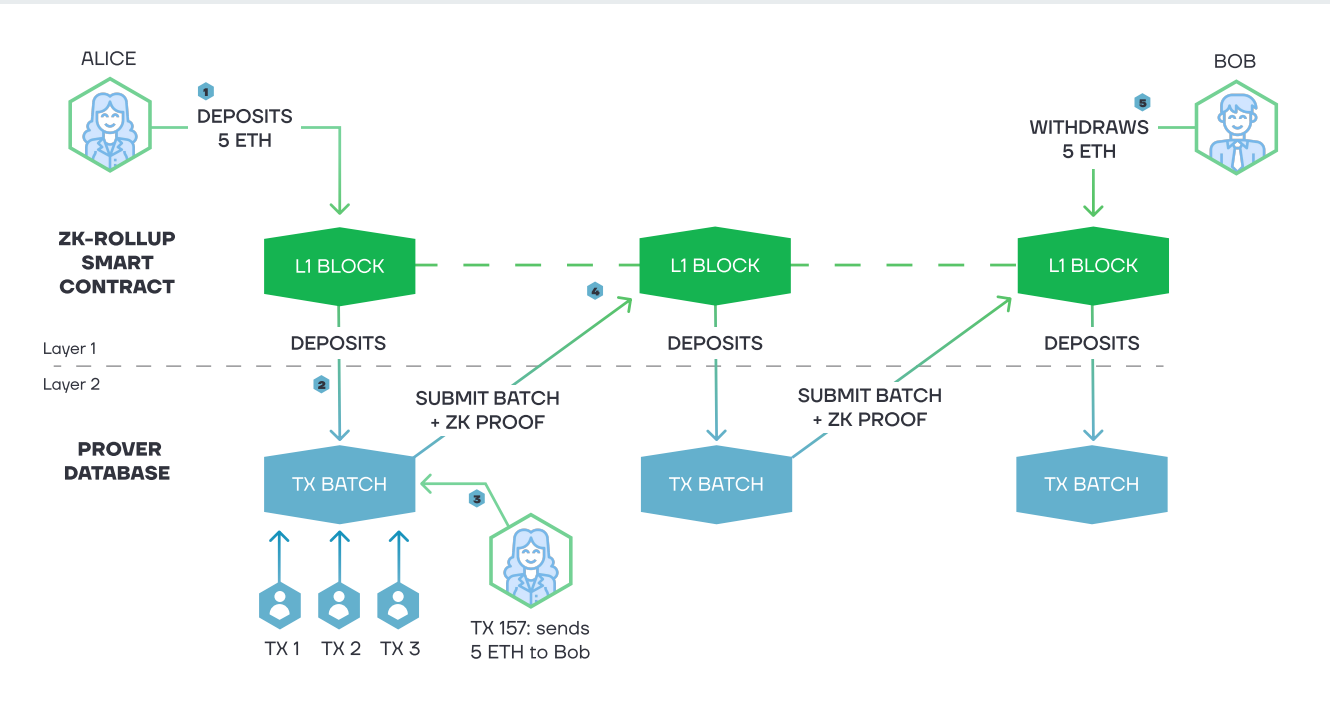


Figure 5: A transaction's life cycle on a zk-rollup. Tx batch refers to a batch of transactions.  
Source: Enabling Blockchain Services for IoE with Zk-Rollups Thomas Lavour, Jérôme Lacan, and Caroline P. C.

However, ZK-rollups come with certain drawbacks, primarily stemming from the use of compilers and new native programming languages. While many developers are familiar with EVMs, they need to invest time and effort to learn how to build dApps on these new codebases. Each block requires separate calculations since transitions between states must strictly adhere to allowed states. This architectural distinction makes the calculations for ZK-rollups significantly different from those performed on the EVM.

The **Ethereum Virtual Machine** is a particular part of Ethereum that complements the distributed ledger technology, on which all blockchains operate. An EVM can be described as a distributed endpoint machine - it facilitates the hashing of smart contract states by creating a value associated with a contract account, according to the consensus mechanism of the Ethereum network. You can think of an EVM as a distributed machine executing smart contract code on a blockchain.

The need for compilers and intermediate languages can also be seen with a simple example. L2 does not generate new addresses for users. Instead, addresses on L2 are mapped to addresses on L1 via a single set of private keys. And to reduce transaction data, the accounts in the ZK- rollup itself are represented by indices rather than addresses to save up space (20 bytes vs. 3 bytes):

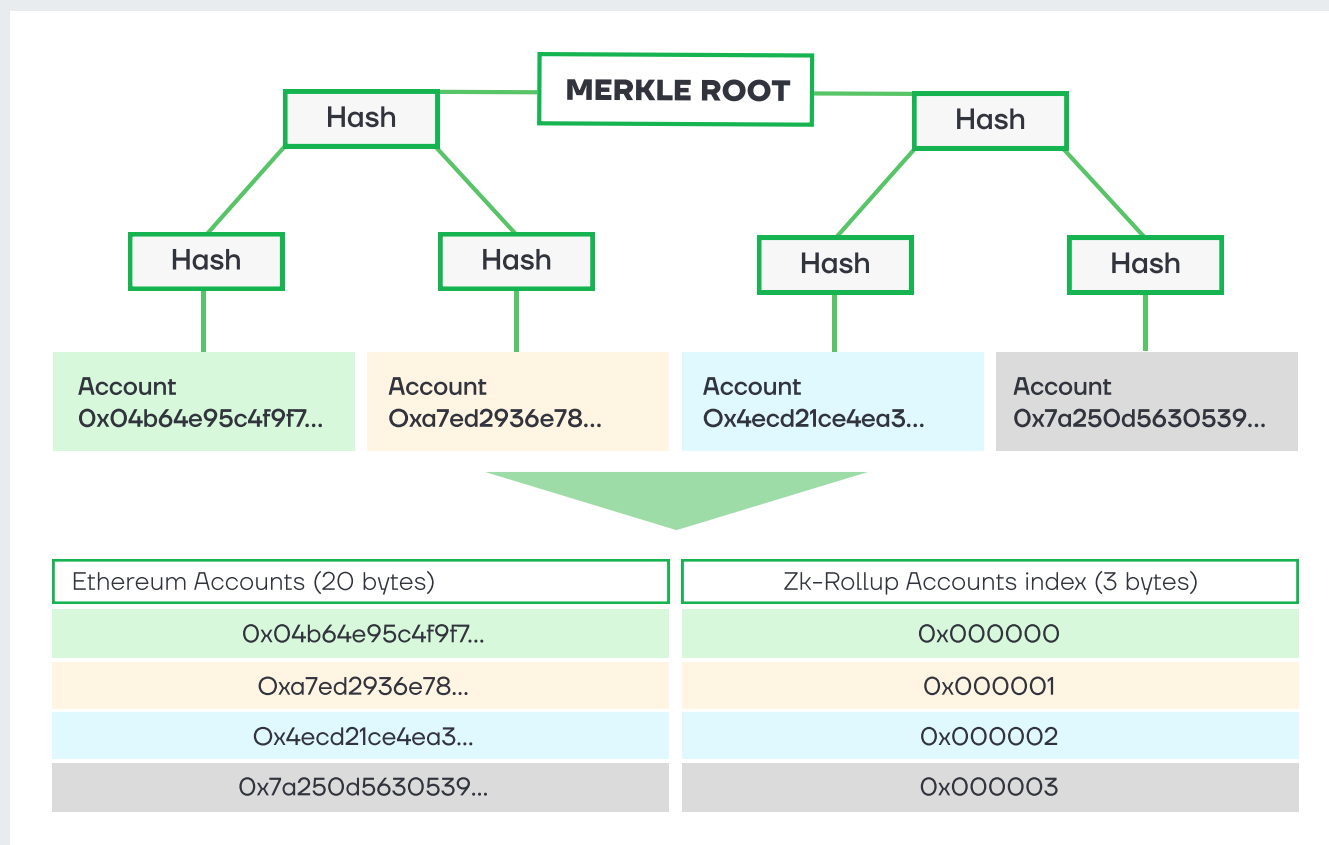


Figure 6: Representation of Ethereum accounts on a rollup.

Source: *Enabling Blockchain Services for IoE with Zk-Rollups* Thomas Lavour, Jérôme Lacan, and Caroline P. C.

The focus is on proving that all transactions are valid and correct. Evidence systems like SNARK and STARK can be used as proof of fraud and validity.

It's also worth remembering that generating proofs and dealing with smart contracts are two completely different things. ZKs can hash data into themselves, but they do not act as virtual machines. And that's where the main difficulty with ZK-rollups lies: If they are highly EVM-compatible, they require vast amounts of power and run slowly, so it's easier to take the generation of ZK-proofs to the off-chain.

On the other hand, if ZK-rollups are fast, they generally require languages other than Solidity. This either leads to creating other tongues and virtual machines, directing the development of applications from scratch, or producing compilers and SDKs for compatibility with EVM and YUL, Vyper, and Solidity languages. It is the biggest drawback of ZK-rollups and why optimistic rollups are currently leading in ecosystem development.



## TYPICALLY, ZK-ROLLUPS ARE BASED ON TWO SMART CONTRACTS DEPLOYED ON ETHEREUM:

- The main smart-contract tracks transaction in blocks. It also monitors and compares the state of the blockchain (balance changes, fulfillment of smart-contract conditions, and so on).
- Verifier smart contract (repeater, sequencer) - verifies proofs with ZK-proofs submitted by block producers.

As a rule, several kinds of nodes in L2 are built on ZK-rollup technology. However, a lot of sources often need clarification on both their names and their functionality, so let's discuss them in a bit more detail:

- **Validators (full nodes)** - store the full blockchain history and verify transactions before they reach the sequencer, saving the sequencer the work of transaction validation. There is some confusion as to what validators and sequencers are responsible for: Starknet provides a clear distinction between validators and sequencers. Meanwhile, according to the ZK-rollup architecture section in the zkSync documentation while zkSync specifies that validators aggregate thousands of transactions into one block and send the cryptographic commitment (root hash) of the new state to a smart contract in the core network along with the cryptographic proof (SNARK).
- **Sequencer** - supposedly responsible for collecting transactions and storing history (full nodes). The sequencers in ZK and optimistic rollups are currently centralised, as they are responsible for the most sensitive part: simplifying transactions and generating blocks to the prover, which already generates the proofs. Starkware and others at ZKR aim to move to a more decentralised sequencer implementation over time. In particular, Starkware hopes that various teams can create sequencers that work for Starknet.
- **Provers (relayers, repeaters)** - generate proofs and are rewarded with network tokens (at least by zkSync and Starkware). A prover running on zkEVM does not execute bytecode but generates proofs, which confirm the correctness of the network state changed after executing smart contracts. Repeaters generate a brief, non-interactive, zero-knowledge argument that compares the state of the blockchain before and after each transaction (i.e., the wallet balance), which reaches the underlying network as a verifiable hash. While almost anyone can act as a relay, they must first zest their funds into the smart contract, which will incentivise them to act in good faith.
- Finally, a ZK-proof confirmation and a list of changes to the contract (without addresses and changes to their balances) are sent to Ethereum. Their state is then **verified** by the accumulation contract (verifier) and then updated to the final state. The verifier runs the verification algorithm with the verification key, the proof and the publicly available input data.

Some ZKRs, Aztec network and zkSync, allow anonymous transactions. However, this is impossible at the protocol level in optimistic rollups since all on-chain data is public. In the case of the sequencer, it is worth noting that other validators in the optimistic rollup network act as 'arbitrators' who can 'declare foul'. They can publish evidence of fraud when necessary to initiate a dispute resolution process. And if the sequencer fails in ZK-rollups, the survivability of the network is usually compromised. No one is immune to hardware failures.

**Vitalik Buterin's guide to rollups from 2021:** Optimistic rollups will probably win for general-purpose EVM computation in the short term, while ZK-rollups will probably be used for simple payments, exchanges, and other application-specific use cases. Still, as ZK-SNARK technology improves, ZK accumulation packages will win for all use cases in the medium to long term.












## TPS

Many L1 and L2 chains measure their TPS as some most significant matters. However, all decentralized solutions have yet to overtake centralized payment systems in the number of transactions processed per second.

And this is normal, as big financial giants centrally control payment networks and can boost them as they want without boundaries. Blockchains are too young and chaotic to have the same orderly operation structure, and blockchain users' security and financial independence are more critical than TPS.

Security, reliability, and transaction costs are characteristics that can give a clearer picture to compare L1 and L2 solutions. We'll cover this topic as well since TPS is definitely of interest to the user who wants to interact with the network.

Today, the Ethereum network can handle between 15 and 45 transactions per second. The maximum has been recorded at around 117 transactions. Rollups are designed to increase throughput to 1,000-4,000 transactions per second, but the actual numbers do not match the claimed numbers. In the long term, Layer 2 can provide much faster services than Layer 1.

	OR	ZKR
EVM - COMPATIBILITY	Mostly native EVM compatibility at the expense of geth.	There is no native EVM compatibility, requiring separate SDKs and compilers. Therefore, developing maximum EVM compatibility is now the primary goal of most ZK-rollups.
PROOFS OF VALIDITY	Fraud Proofs are formed only when it is necessary to prove fraud. Do not require significant calculations.	Zero-knowledge proofs are generated using complex cryptographic calculations and require significant computation.
TRANSACTION FEES	<div>Fixed gas cost per batch ~ <b>40,000</b> gas for a lightweight transaction that changes the value of the state root.</div> <div><div><div></div><div>send</div><div>\$ 0.04</div></div><div><div>swap</div><div>\$ 0.11</div></div></div> <div><div></div><div>send</div><div>\$ 0.1</div></div> <div><div>swap</div><div>\$ 0.14</div></div> <div><div></div><div>send</div><div>\$ 0.09</div></div> <div><div>swap</div><div>\$ 0.23</div></div> <td><div>Fixed gas cost per batch ~ <b>500,000</b> (for transaction with ZK-SNARK verification).</div><div><div><div></div><div>send</div><div>\$ 0.14</div></div><div><div>swap</div><div>\$ 0.34</div></div></div><div><div></div><div>send</div><div>\$ 0.45</div></div><div><div>swap</div><div>\$ &gt;1</div></div><div><div></div><div>send</div><div>\$ 0.2</div></div><div><div></div><div>send</div><div>\$ 0.35</div></div><div><div>swap</div><div>\$ 1.34</div></div></td>	<div>Fixed gas cost per batch ~ <b>500,000</b> (for transaction with ZK-SNARK verification).</div> <div><div><div></div><div>send</div><div>\$ 0.14</div></div><div><div>swap</div><div>\$ 0.34</div></div></div> <div><div></div><div>send</div><div>\$ 0.45</div></div> <div><div>swap</div><div>\$ &gt;1</div></div> <div><div></div><div>send</div><div>\$ 0.2</div></div> <div><div></div><div>send</div><div>\$ 0.35</div></div> <div><div>swap</div><div>\$ 1.34</div></div>
TRANSACTION VALIDATION	Up to 1 week, you can publish proof of fraud and cancel the withdrawal, if necessary.	~ 10 minutes, immediately after forming and transmitting a transaction packet.
SECURITY	Transactions are initially assumed to be correct, so verifiers and validator whitelists are required.	ZK-proofs generate security on a high level.
TPS	<b>500 TPS - 2000 TPS</b>	<b>2000 TPS - 100.000 TPS</b>



**AJ PARK**  
Founder of Radius



Radius is a shared sequencing layer that protects users against harmful MEV and censorship, while enabling rollups to maximize profits in better ways — all within a trustless environment.

Two main blockchain-related problems can be addressed through zero-knowledge proofs: scalability and privacy. Scalability is addressed through solutions like ZK-rollup, which uses zero-knowledge proofs to validate state transitions resulting from transactions' execution off-chain in Layer 2. Privacy involves proving the validity of sensitive information while concealing it, and it complements the trustworthiness of information by using zero-knowledge proofs, such as selective disclosure in DID, where only certain information is revealed.

However, these two aspects are just a subset of the many things that can be accomplished with zero-knowledge proofs. To further explore their potential, it is necessary to understand the underlying principles and properties of zero-knowledge proofs that enable scalability and privacy. Zero-knowledge proofs can be used for proving the "integrity of computations," which means demonstrating that certain computations have been performed correctly based on "mathematical" principles, without relying on specific third parties. State transitions required for scalability and proving the trustworthiness of partial information for privacy fall under these computations. The utility of zero-knowledge proofs can be maximized depending on the type of computations being performed. Additionally, since it is based on mathematics, it is possible to build trustless protocols that do not require trust in third parties. Trust assumptions, which are assumed in crypto-economics or some solutions, can lead to significant issues if that trust is broken, but ultimately, these can be addressed through zero-knowledge proofs. By applying computations that validate zero-knowledge proofs themselves, the utility of zero-knowledge proofs is further enhanced. Through a technique known as Recursive ZKP, even if a large number of off-chain computations need to be proven, the verification can be kept constant, minimizing on-chain verification operations (i.e., with fixed costs) while maximizing the number of computations that can be proven.

However, zero-knowledge proofs are by no means free. The mathematical computations required to prove the integrity of computations are generally highly computation-intensive, thus requiring significant resources and time. When constructing zero-knowledge proof-based solutions, it is crucial to clearly identify the responsible party for these costs to ensure sustainability. Simply relying on the advantages provided by zero-knowledge proofs without considering who will bear the costs and how those costs will be made up is not a viable long-term approach. These considerations must be included as part of the solution.

Radius defines a centralized sequencer for rollups as one of the critical problems that can be solved using zero-knowledge proofs, and it is currently building a solution with its own cryptography scheme. Radius has introduced an Encrypted mempool to address censorship and harmful MEV issues caused by centralization. This approach encrypts transactions to prevent these problems. However, since the transactions are encrypted, the integrity of the transactions themselves cannot be verified. To address this, Radius aims to use zero-knowledge proofs to prove the integrity of the encrypted transactions. For example, it can verify if the encryption was done correctly and if the signatures of the encrypted transactions are valid. Moreover, this trustless sequencer can make a profit by extracting benign MEV from its network, so the cost to do with zero-knowledge proof can be covered for its sustainability.

With recent technological advancements that have increased the practicality of zero-knowledge proofs, Radius will continue to experiment with the potential of zero-knowledge proofs to solve various issues, such as interoperability between rollups.

Backed by:

**#HASHED**

 **Superscript**

 **AMBDA**  
CLASS

 **crypto.com** | **CAPITAL**



# ZK-SNARK AND ZK-STARK PROOFS

Two main types of ZK-proofs are ZK-SNARKs and ZK-STARKs, both of which play a crucial role in addressing the challenges posed by Ethereum scaling and optimistic rollup.

The key distinction between ZK-SNARK and ZK-STARK lies in their cryptographic models for constructing proofs. ZK-SNARK is well-established and provides a high level of security in terms of proof integrity. ZK-SNARK emerged earlier during the Zcash era and has garnered a considerable number of developers who possess expertise in its implementation. These developers provide assurances regarding the security of ZK-SNARK.

On the other hand, ZK-STARK is still an area of active research and development, with practical implementation and real-world applications being actively explored. ZK-STARK enables the off-chain transfer of calculations to a single STARK prover, with the on-chain STARK verifier ensuring the integrity of those calculations. While STARK proofs are more challenging and costly to verify compared to SNARK, they offer superior throughput and scalability compared to ZK-SNARK.

STARK certificate generation is approximately ten times faster than SNARK. One notable distinction between ZK-SNARK and ZK-STARK is their behavior under increased computational load. With ZK-SNARK, as the complexity of computations (such as the number of transactions) increases, the required load also increases linearly. In contrast, ZK-STARK demonstrates a more efficient scaling property, where the load does not increase as significantly with increasing computation.

Another advantage of STARK is its inherent quantum resistance, offering protection against potential future threats from quantum computers. While SNARKs are also exploring quantum resistance with developments like PQ-SNARK, practical testing and implementation of quantum-resistant SNARKs are still ongoing.

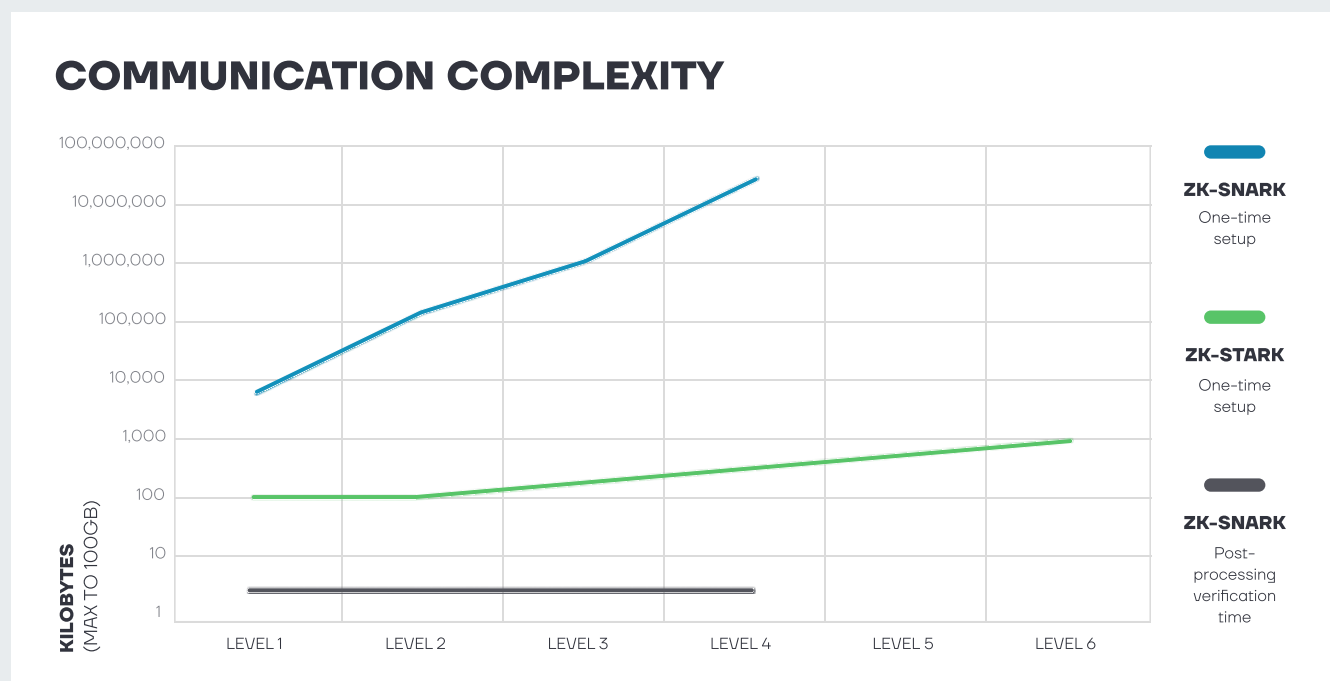


Figure 7: Communication complexity zk-SNARK vs zk-STARK

Source: ZK-STARKs — Create Verifiable Trust, even against Quantum Computers, Adam Luciano

Also, ZK-STARK's transparency eliminates the requirement for a trusted setup, strengthening its security and making it a highly desirable option in the field of zero-knowledge proofs. By removing the need for an initial trusted ceremony, ZK-STARK offers a more robust and self-contained solution for secure and scalable knowledge proofs.

**Trusted setup** is the process of creating a Common Reference String (CRS), through which the proving and verifying parties know that they are using the same statement. It is a piece of data that is used every time the cryptographic protocol is run. It requires some secret information to create this data; "trust" comes from the fact that some person or group has to create these secrets, use them to create the data, and then publish the data and forget about the secrets.

While some SNARKs do require a trusted setup ceremony, the development of transparent SNARKs has addressed this concern by providing a trustless alternative. These transparent SNARKs enable the generation of structured proving keys without relying on any trusted setup, bolstering the security and decentralized nature of the SNARK-based solutions. Specifically, many SNARKs (e.g., Groth16, PlonK, Marlin, Bulletproofs, Nova) rely on the assumption that discrete logarithms are difficult to compute, but they are not post-quantum secure (non-PQ).

However, it is worth noting that STARK has a significant drawback compared to SNARK: the size of its proofs. ZK-STARK proofs can occupy a substantial amount of memory, ranging from 100KB to 250KB. Consequently, efforts are underway in various projects to reduce the size of STARK proofs. For instance, initiatives like Halo and SuperSonic have achieved proofs as small as 10KB or less.

Additionally, data suggests that SNARK requires approximately four times less gas than STARK, despite the potential presence of more packetized data in STARK.

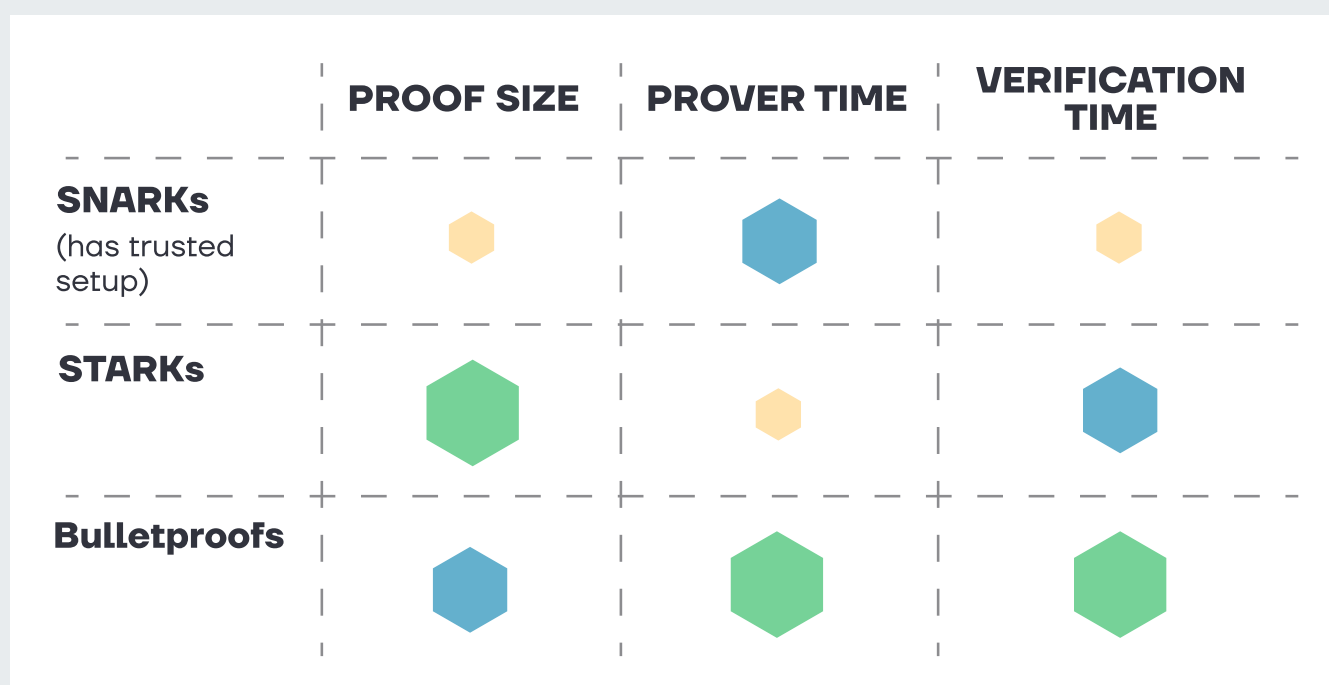


Figure 8: SNARKs, STARKs and Bulletproofs comparison

Source: StarkNet Sheds a Light on a New Direction for ZK-Rollups, Jaewon Kim



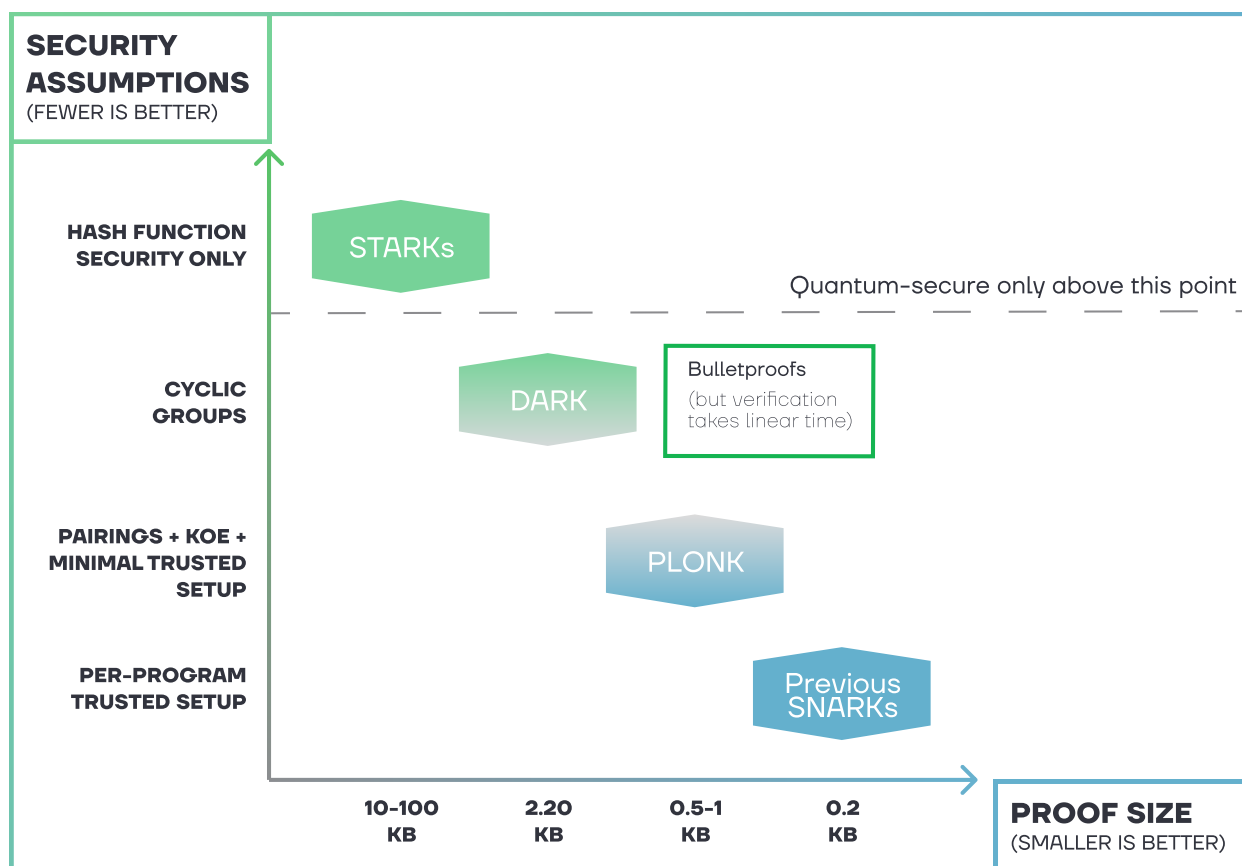


Figure 9: zkEVM types comparison

Source: The different types of ZK-EVMs, Vitalik Buterin

Several teams are actively engaged in enhancing ZK-SNARK technology:

- **Groth16** is the first implementation of ZK-SNARK, introduced in 2016 and remains the fastest and smallest known ZK-SNARK and is used in Zcash. However, its small size may be a disadvantage as well, as it allows you to write less data.
- **Sonic** appeared in 2019. It supports a universal and updatable general reference string. Sonic proofs have a constant size, but verification is expensive. In theory, multiple proofs can be verified in a batch mode to improve performance, greatly improving throughput, but that's the only way that Sonic can provide good speed. Sonic also gets a versatile and upgradable CRS, which improves safety.
- **Plonk** is an improved version of Sonic, with a five times faster prover time and a smaller proof size. It offers better prover time but worse runtime than Sonic. However, it is still slower than Groth16 in verification time and larger in proof size. Despite the increase in the size of the proof by 2.5 times, Plonk consumes only 10% more gas than the Groth16 (0.2kb vs. 0.5kb). (13) It is used in all recent iterations of ZK-SNARK (zkSync, Scroll, Aztec, Mina Protocol, Dusk). Plonk can be considered the most dynamically evolving variant of ZK-SNARK at the moment, as there are many different variations: fflonk, turbo PLONK, ultra PLONK, plonkup, and the recently introduced, plonky2.
- **Marlin** is considered by some researchers as a further development of Plonk, but it was actually introduced in 2019, around the same time as Sonic and Plonk. It has common authors with Sonic and plonk. It has common authors with Sonic and is positioned as a solution suitable where batch processing cannot be used. Marlin is said to have 10 times better prover time and four times faster verification time than the original Sonic.

- **Fractal** – introduced in 2020, is an extension of Sonic and Marlin. It requires no trusted installation and is quantum resistant, as Fractal is based on hash functions for which quantum attacks are currently feasible. This all brings this SNARK variant considerably closer to STARK. Unfortunately Fractal has a larger proof size, which increasing gas consumption accordingly.
- **Brakedown, Orion** – FRI-based proofs, faster prover, but longer proofs. These are the latest implementations of ZK-SNARK. Unlike Breakdown, proposed by Golovnev in 2021, Orion has a much smaller proof size, which has a significant impact on block space and gas consumption. The scheme is based on a linear code coding scheme and shows that the second argument proof with zero disclosure is the same as the message in the linear code. But the proof size is still much larger than that of SNARK, derived from Growth16.

	PROOF SIZE	PROVER TIME (PROOF CONSTRUCTION)	VERIFIER TIME (PROOF VERIFICATION TIME)	TRUSTED SETUP	VERIFIER TIME (PROOF VERIFICATION TIME)	QUANTUM RESISTANCE
BULLETPROOF	2.5kb	~30-100 sec	~1-5 sec	No	No	No
ZK-STARK	45-200kb	~ 1.6-4 sec	~16-40 ms	No	No	Yes
GROTH16	0.13-02 kb	~1-2 min	~1-10 ms	Yes	323mb	No
SONIC	1 kb	~134 sec	~0.72 ms	Yes, updatable	600mb	No
PLONK	0.51 kb	~5 sec	~1 ms	Yes, updatable	16mb	No
MARLIN	1 kb	~70 sec	~8 Ms	Yes, updatable	16mb	No
FRACTAL	60-200 kb	~3-6 min	~4-10 ms	Yes, updatable	No data	Yes
BRAKEDOWN	~10mb	~3.1 sec	~1 sec			Yes
ORION	~1.5mb	~3.09 sec	~1 sec			Yes

Source: Polaris: Transparent Succinct Zero-Knowledge Arguments for R1CS with Efficient Verifier, Shihui Fu and Guang Gong. FRACTAL: Post-Quantum and Transparent Recursive Proofs from Holography, Alessandro Chiesa, Dev Ojha, Nicholas Spooner. Zk-SNARKs vs. Zk-STARKs vs. BulletProofs? (Updated), Paul Razvan Berg. Zero-Knowledge: PLONK Demo, Mels Dees

**Note:** the speed and size values are highly dependent on such a parameter as constraints (gates), and unfortunately, the sources do not indicate at what particular value of constraints certain data were obtained. Judging by the comparison of data in various sources, the standard value is  $2^{16}$  constraints (gates). The more constraints (gates) – the more time and size of evidence grow. It is also very much dependent on the hardware used – the number of cores and processor threads, which are usually not specified in comparisons, and it is impossible to know if the same hardware was used. The data should therefore be considered approximate. Based on the comparison of the data, machines with 24-32 threads and 32GB of RAM were commonly used.

**By Eli Ben-Sasson, StarkWare:** The argument over which argument system to use is far from over. But at StarkWare we say: For short arguments, use Groth16/PLONK SNARKs. For everything else, there's symmetric STARKs.

## EVM COMPATIBILITY FOR ZK-ROLLUPS

Many rollups initially rely on their own programming language, limiting the influx of developers. Most application developers on the Ethereum network are used to writing in Solidity and have trouble writing smart contracts in existing L2s. But in general, all ZK-rollups run on virtual machines called zkEVMs because EVM smart contracts don't just run, but they must also be compatible with ZK-proof computation.

EVM compatibility is currently one of the main goals of all rollups on their way to expanding the ecosystem. New SDKs and compilers have been actively introduced in the past year, and work continues on solutions that will help deploy dApps on L2 as conveniently and efficiently as on L1.

- **EVM interoperability:** you can translate Solidity/Vyper code into byte-code of the virtual machine, and then inside the schema, you confirm the validity of the execution trace.
- **EVM-equivalence:** you can translate or interpret the EVM byte-code into your virtual machine byte-code and then confirm the validity of the execution trace inside the schema.
- **For a full-scale zkEVM,** you confirm the validity of the EVM execution trace within the blockchain.

Of the running ZK-rollups of type 4 EVM compatibility (about types of compatibility below), zkSync has the most developed EVM compatibility thanks to the use of intermediate solutions like compiling to Yul, an intermediate language, followed by compiling to zkEVM bytecode via LLVM. It is worth noting that while using intermediate solutions does promote EVM interoperability of the rollups, it does add complexity to the application deployment process, and the logic of operation may sometimes suffer from this



**ARIS ZARIMPAS**  
DevRel of Hashstack



Hashstack provides a permissionless zk-native money market protocol enabling secure under-collateralised loans (up to 3x the collateral) to the crypto retail.

There are two primary types of ZK technology being utilised in blockchain: ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) and ZK-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge). While they serve a common purpose, there are key differences that led to the creation of passionate communities around each of them. In brief, SNARKS, as the first approach, have more docs, libraries, devs, and projects under them. In technical terms, they require a smaller proof size and a trusted set up. STARKS, on the other hand, require more gas and are more difficult to learn, but they do not need a trusted set up and are quantum resistant (once quantum computers are out). It's useful to mention that ETH Foundation has awarded a big grant to StarkWare which uses the STARKS approach.

Expanding to the variety of ZK solutions there is one more major category. Zk-EVM (with its variations) and non EVM set up. A zero-knowledge Ethereum Virtual Machine (zkEVM) is an EVM-compatible virtual machine that enables zero-knowledge rollups. This brings the existing Solidity-based smart contract logic, token standards, and tooling to a highly scalable and secure layer 2 environment. As a result, developers can easily build applications using familiar tools and bring existing dApps and smart contracts to the new environment. In this category we can find the majority of solutions like zkSync, Polygon, Scroll etc. A key representative for the non EVM paradigm is Starknet. They use their own language called Cairo instead of Solidity. As it is newer, Cairo faces the challenges of every new technology under development. Less documentation, smaller community, frequent updates and some disbelief from the outsiders. On the other hand Cairo is claimed to be more secure, flexible, composable and faster than Solidity, making it ideal for the ZK-rollups.

Zero-knowledge (ZK) technology is a type of encryption that enables parties to demonstrate the validity of information without revealing the actual information itself. Although the concept counts decades, it regained traction recently as an add-on in blockchain technology and is mostly associated with the ZK-rollups (currently, the most promising Ethereum scaling solution). There are many teams working on new and existing projects that adopted this groundbreaking tech, including Starknet, zkSync, Scroll, Aztec, Loopring, Mina and Polygon. The approaches may vary, but the value proposition is common. Higher tps, lower tx fees, enhanced privacy and security in cryptocurrency transactions. It won't be long until we see most - if not all - of the major blockchains, rolling out a zk version. The hype is huge, the use cases are obvious, and we are still early.



- **Type 1 ZK-rollups**, which offer full Ethereum compatibility, maintain the same logic, hashes, and architecture without the need for compilers or modifications. Ethereum network clients can be seamlessly used without any changes. One example of such a rollup is Taiko. However, a drawback of full EVM compatibility is that it can impact the performance of ZK functionality and require significant computational resources for proof calculations. To address this challenge, the development of solutions for parallelizing calculations or dedicated ASIC devices might be necessary in order to achieve efficient and scalable ZK-rollup operations.
- **Type 2 ZK-rollups** offer full EVM equivalence, but with slight differences in the block structure, state tree, and hash functions compared to Ethereum. These differences are not accessible by the EVM itself, so the logic of applications remains unchanged, requiring only minor modifications to Ethereum executable clients. Type 2 rollups, such as Scroll and Polygon Hermez, provide access to the entire Ethereum infrastructure. However, a drawback of type 2 ZK-rollups is the generation time for ZK-proofs, which can still be relatively long. To mitigate this issue, it may be necessary to increase gas costs for resource-intensive operations, ensuring efficient resource allocation for "heavy" operations.

“



**CHICHI HONG**  
Co-founder of  
ScalingX



Zero-Knowledge proof (ZKP) is on the brink of revolutionizing how we approach privacy, security, and trust in the digital era. These remarkable constructs not only provide privacy-preserving solutions for handling sensitive data but also possess the capacity to amplify the efficiency, scalability, and security of blockchain networks, even when dealing with ordinary data transmission and verification.

Industries that handle sensitive information, such as blockchain, finance, and healthcare, stand to gain significant benefits from the transformative power of ZKP. ZKP offers a robust tool to maintain privacy while ensuring secure and efficient data transactions within blockchain technology. By leveraging ZKP, blockchain networks can safeguard against fraudulent activities and maintain the integrity of the entire system. As the utilization of blockchain technology continues its rapid expansion, the significance of zero-knowledge proofs is poised to soar.

While some other applications such as ZK-rollup and zkML are currently in their early stages, it is only a matter of time before they mature and usher in a vibrant new ecosystem of ZK-powered applications. This new wave of applications will be the key to a future where privacy and transparency harmoniously coexist.

ScalingX is a global accelerator across Singapore, Hong Kong and San Francisco dedicated to the development of Web3 and blockchain technologies, with a focus on Zero-Knowledge Proof (ZKP) technology. Our goal is to advance the adoption of blockchain technology around the world through investments. We support early-stage Web3 startups by helping them with talent recruitment, networking, fundraising, project incubation, PR and branding, community building, and more. We are fully committed to building a more scalable, transparent, secure, and decentralized network of tomorrow.

”

- **Type 3 ZK-rollups** offer partial EVM equivalence, where certain functions that are challenging to implement in zk-EVM may be absent, and there are differences in contract code handling and the stack. However, a significant drawback of type 3 rollups is the emergence of notable differences. While they maintain compatibility with most EVM applications, it becomes necessary to rewrite the logic of some applications to adapt to these differences. This requirement adds complexity and additional development efforts.
- **Type 4 ZK-rollups** necessitate recompilation of high-level language code into a ZK-compatible language, which may require additional tools and effort to make EVM applications compatible with the ZK virtual machine. While this type allows for efficient and speedy proof generation, the need for compilers and language translation introduces additional complexity and overhead for EVM applications looking to leverage ZK-rollup technology.

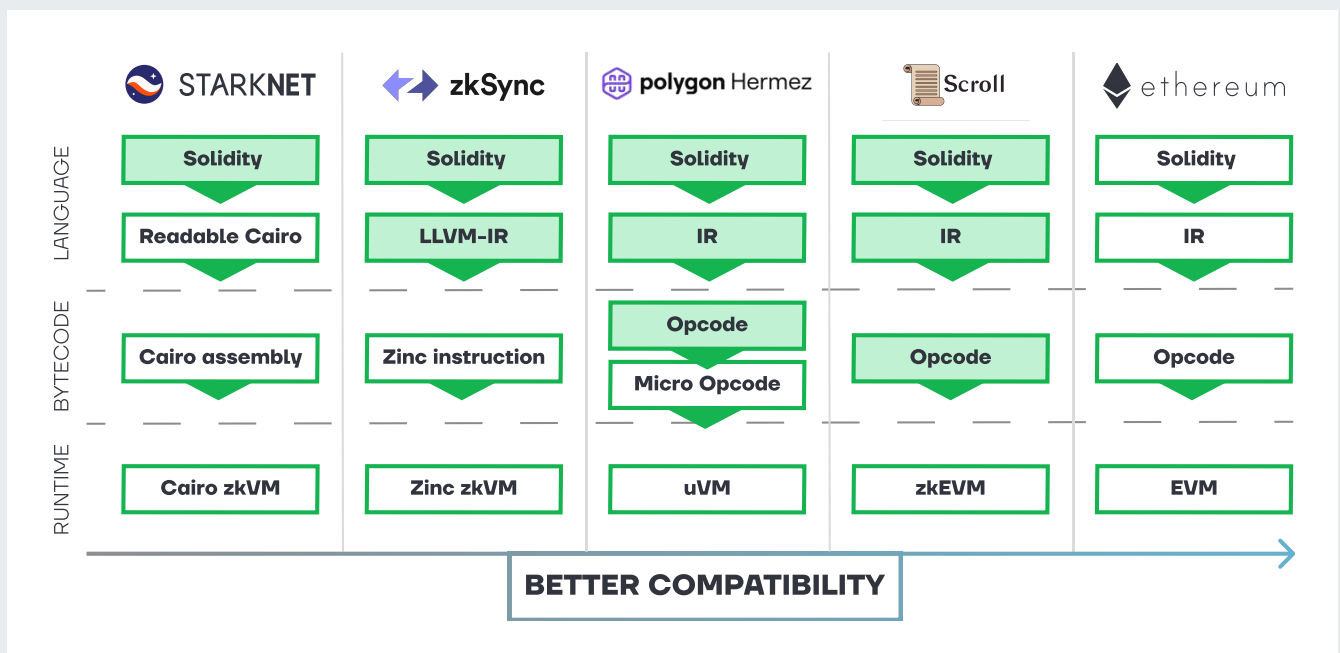


Figure 10: Overview of zkEVM projects featuring StarkNet, zkSync, Polygon Hermez, and Scroll

Source: zk, zkVM, zkEVM and their Future, msfew



# 7 ZK-ROLLUP ECOSYSTEM

## I. ZKSYNC

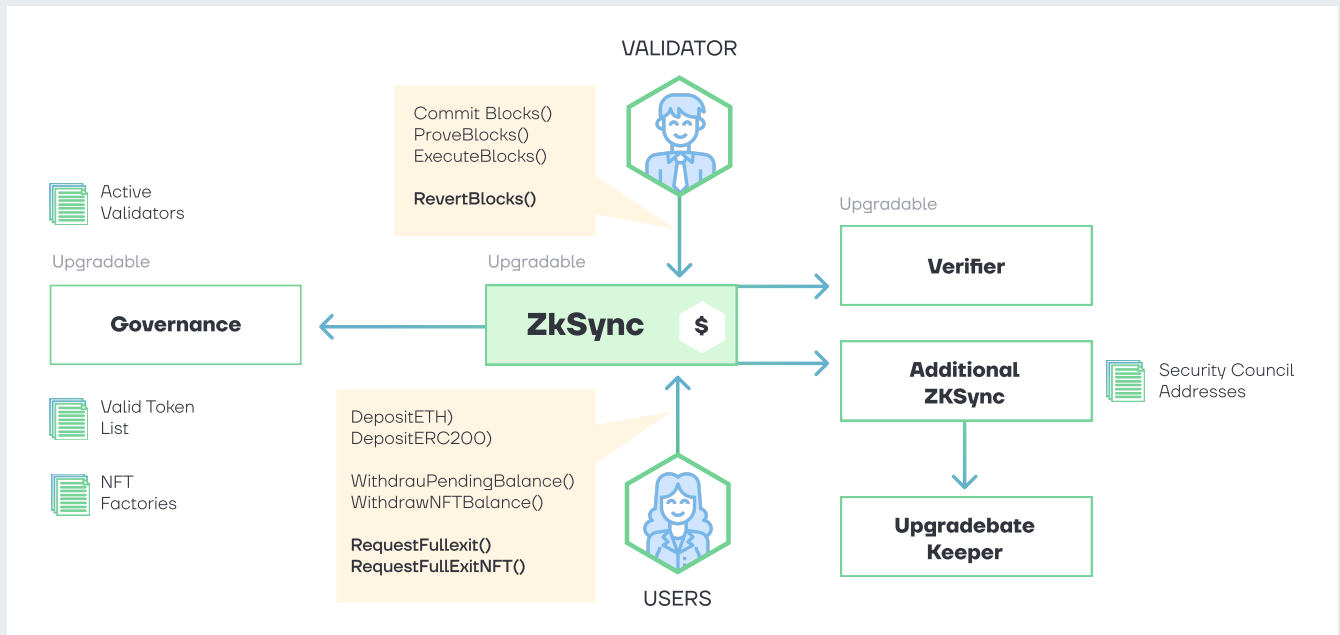


Figure 11: zkSync architecture  
Source: L2BEAT

Matter Labs, founded in 2018, is working on zkSync and first introduced the idea in 2019. zkSync runs on ZK-Snark, and has, according to the developers, 99% compatibility with EVM. Solidity and Vyper require compiling to Yul, an intermediate language, and then using LLVM to compile to zkEVM bytecode. zkSync supports its ZKP-optimized Rust-like language, Zinc. On March 24, 2023, Matter Labs launched zkSync Era, an alpha version of the L2 scaling solution, on the Ethereum core network.

“



**BALAL KHAN**

Co-founder and Head  
of Growth at ZKEX.com

Omni-chain interoperability will be revolutionized with ultra-secure ZK bridges and middleware that use mathematical verification rather than game theory to secure hundreds of billions of dollars of cross-chain transactions. New solutions from Succinct, Electron Labs, Polyhedra, and zkLink will go live this year and enable the aggregation of liquidity and seamless movement of crypto assets across different L1 blockchains and L2 networks. Trustless, zero-knowledge secured protocols that use cryptographic validity proofs to verify cross-chain transactions could well see an end to bridge hacks that caused \$2.5b of losses last year.



ZKEX is a multi-chain  
DEX secured by zero-  
knowledge proofs.

We also predict developers will decide to build multi-chain dApps on multiple Ethereum ZK-rollups, namely StarkNet, and new zkEVMs from zkSync, Scroll, Polygon, and Linea simultaneously. The ease with which dApps can be re-deployed on multiple ZK L2 networks has been dramatically simplified, with re-builds taking only a few weeks as opposed to months previously.

In 2023, get ready for a wave of innovation for zero-knowledge secured interoperability. For crypto users and institutions, this means easier, safer, and cheaper cross-chain transactions that will open access to liquidity in different blockchains and remove barriers for people to use decentralized finance products.

”

Below is a schematic that shows the zkSync modules and their relationships:

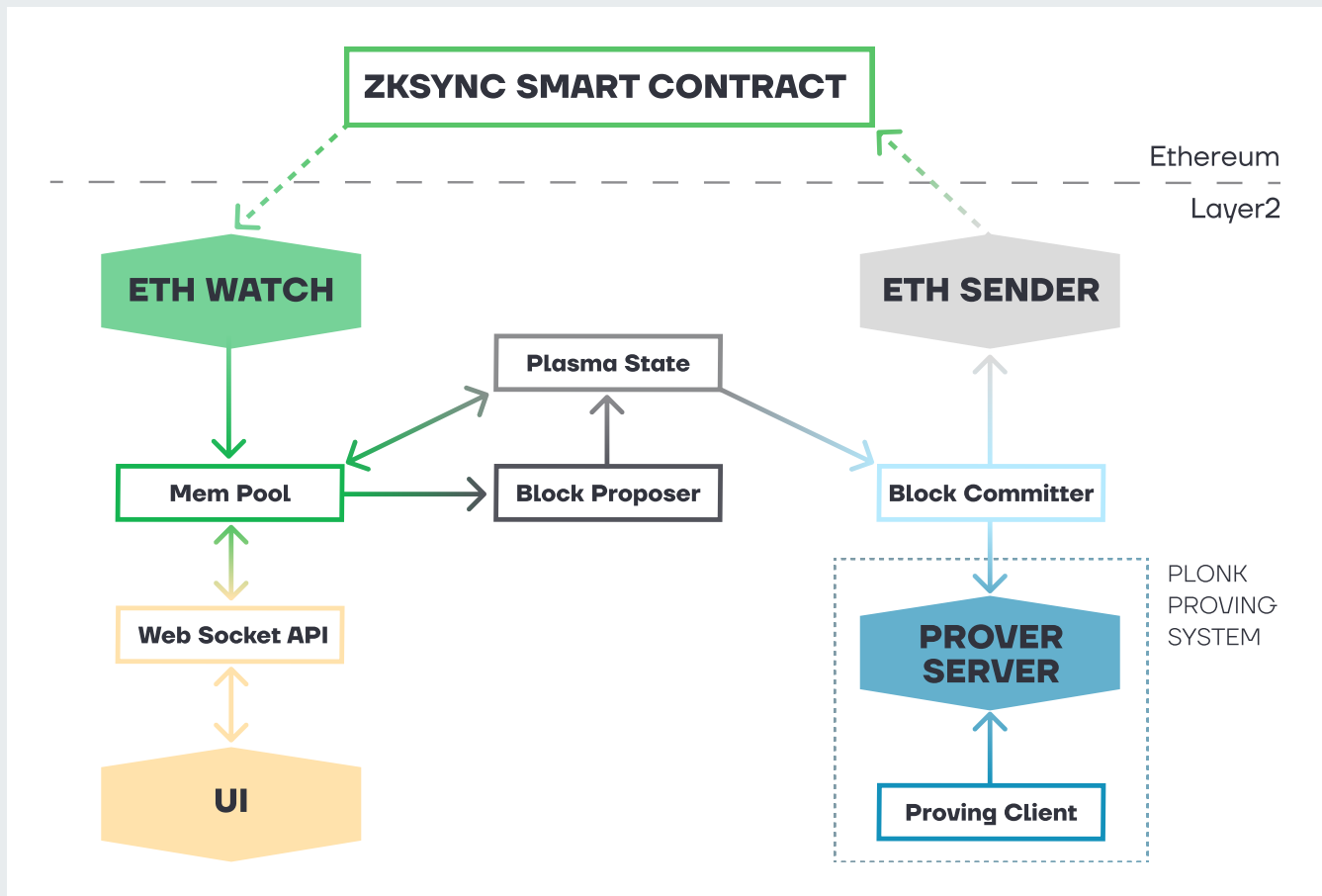


Figure 12: zkSync modular function and inter-relationship

Source: L2 — Deep into zkSync Source Code, Tapdoor-Tech

## ARCHITECTURE:

- **zkEVM:** EVM-compatible ZK-rollup engine, the only solution with L1 protection and support for Solidity smart contracts.
- **zkPorter:** a standalone data availability system with two orders of magnitude more scalability than storage packages.
- **ZkSync main contract:** main storage contract. The operator captures blocks, provides zkProof, which is confirmed by the Verifier contract, and handles withdrawals (executes blocks).
- **Verifier** implements the logic of zkProof verification.
- **UpgradeGatekeeper:** The contract that implements the upgrade mechanism for Governance, Verifier and ZkSync\*\*.
- **Governance** stores a list of block makers, NFT factories and white-listed tokens.
- **Full Nodes:** zkEVM bytecode pre-execution environment, filters out explicitly invalid transactions, 1. Executes transactions in the mempool and generates blocks.
- **Provers** get proofs for blocks and generates ZK-proofs, parallel proof generation is possible.
- **Interactor** - a tool to connect to ETH L1, calculate commission, ZKP generation costs and gas prices in L1.

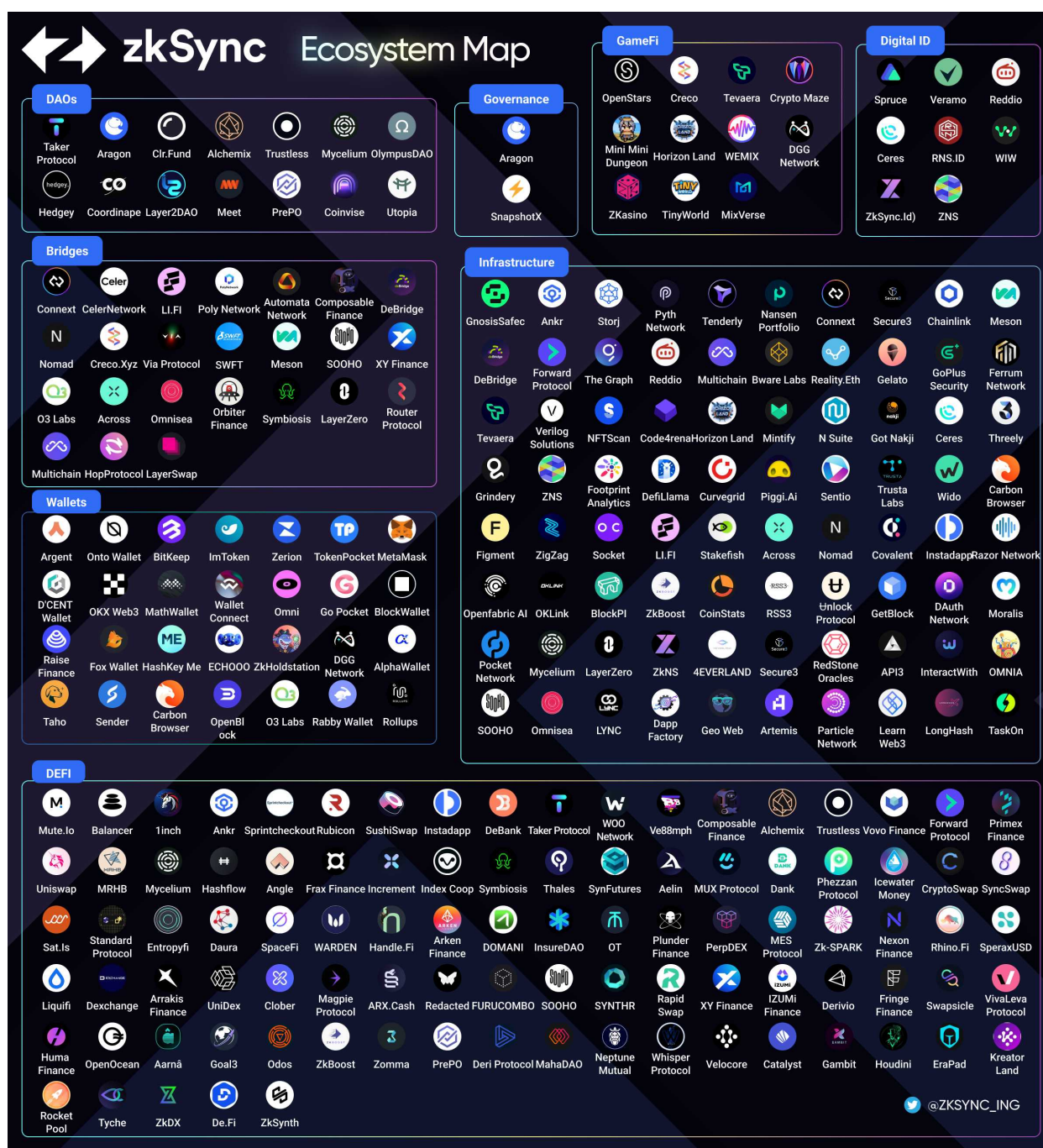


Figure 13: zkSync ecosystem.

Source: ZK Sync Rater

Since zkSync is highly compatible with EVM, many multichain and cross-chain applications run on it. The technology is used in many large projects, including Chainlink, SushiSwap, Uniswap, Aave, Argent, 1inch, and Gnosis.

The zkSync ecosystem currently consists of 223 projects that fall into categories like DeFi, wallets, infrastructure, payments, public goods, social, gateways/CEX, bridges, games, DAO, NFT, governance, privacy, digital ID, and tools. Despite the technology's versatility, zkSync is mostly used in decentralized finance.

## ONCHAIN ACTIVITY AND TVL

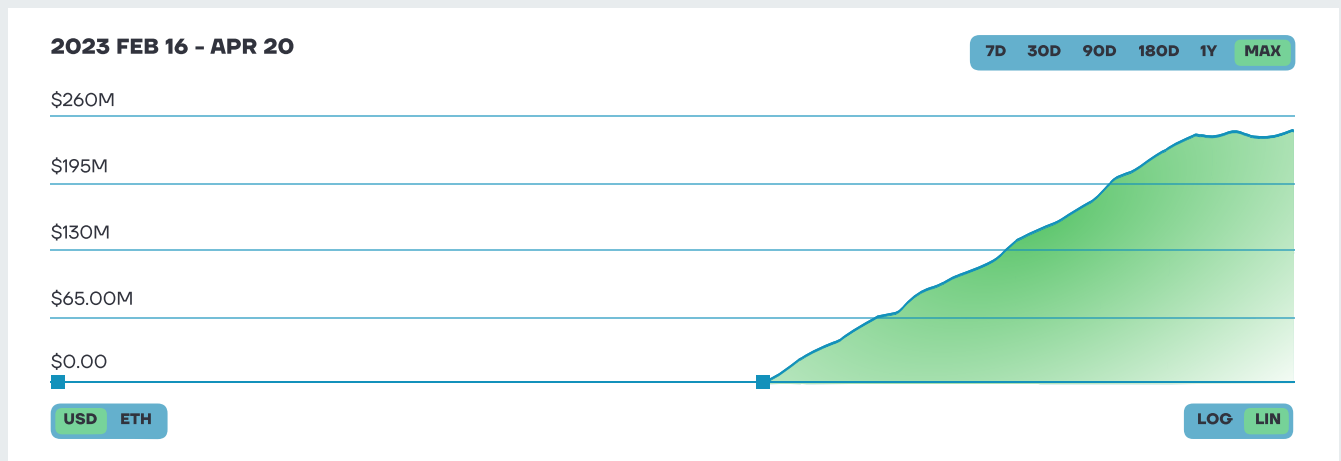


Figure 14: zkSync TVL activity

source: L2BEAT

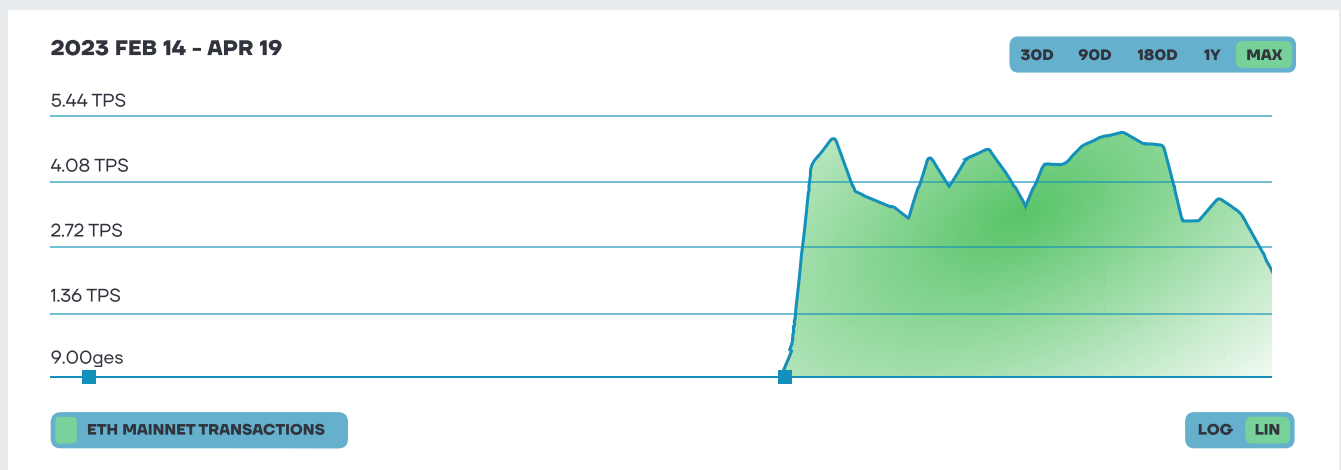


Figure 15: zkSync network activity

Source: L2BEAT

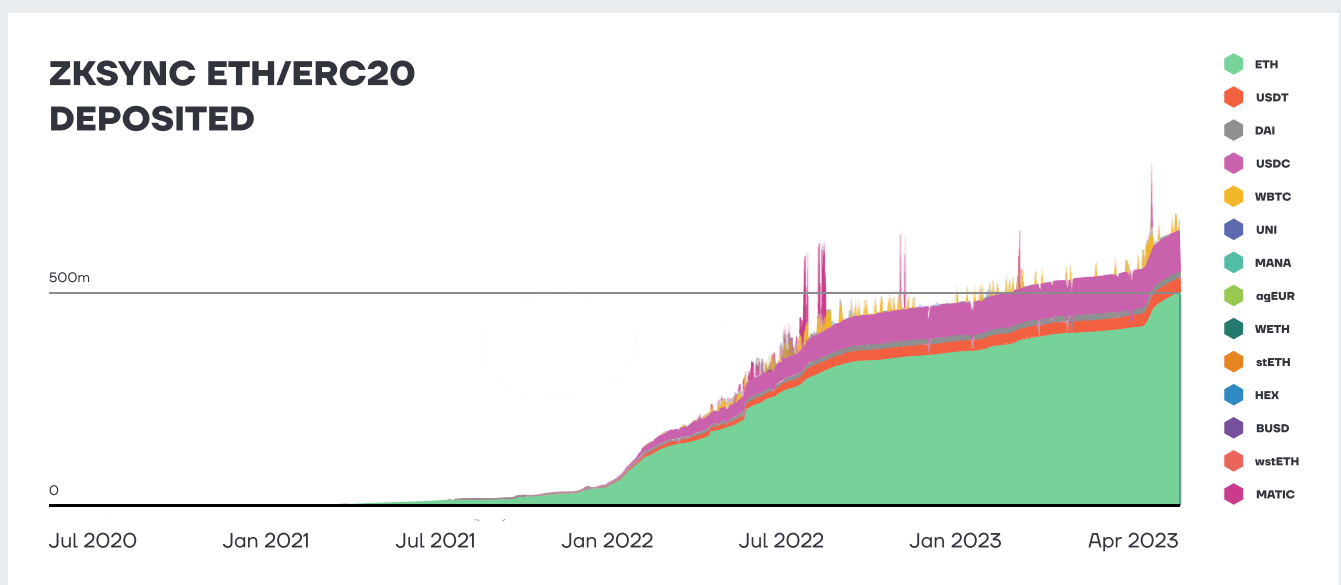


Figure 16: zkSync ETH/ERC20 Deposited

Source: Dune Analytics

## FUNDRAISING AND INVESTORS:

zkSync has raised a total of \$258 million, although some sources claim the amount is closer to \$400mn. This likely includes a \$200 million investment from BitDAO obtained for the development of the ecosystem, bringing the total to \$458 million.


- **September 2019: Seed**, \$2M
- **February 2021: Series A**, \$6M Placeholder, 1kx, Coinbase Ventures, Curve, Aave, Dragonfly, Union Square Ventures
- **November 2021: Series B**, \$50M from Andreessen Horowitz, Placeholder, Dragonfly, 1kx, Blockchain.com, Crypto.com, Consensys, ByBit, OKEx, Alchemy, Covalent, BECO Capital, and joined by the founders and leadership of AAVE, Paraswap, Lido, Futureswap, Gnosis, Rarible, Aragon, Liquity, Celer, Connex, Perpetual, Euler, Opium and 70 more investors
- **November 2022: Series C**, \$200 million, Blockchain Capital, Dragonfly, LightSpeed Venture Partners, Variant, Andreessen Horowitz.

“



**MATTÉO GEORGES**  
CEO of Pragma



in partnership with  **STARKWARE**

Pragma is the first provable oracle, leveraging STARK proofs to deliver data to zk-rollups.

When discussing ZK-proofs, the significance of timing is often overlooked. The concept of ZK-proofs was initially conceived in 1985 by Shafi Goldwasser, Silvio Micali, and Charles Rackoff, meaning nearly four decades have passed since their inception. For more than 30 years, these proofs remained confined to the realm of elaborate mathematics, devoid of practical applications.

However, with the emergence of blockchain technology, ZK-proofs have finally found their purpose, particularly in enhancing scalability and privacy. Returning to the subject of timing, what we are witnessing now is an exponential surge in the adoption of ZK-proofs, following a relatively sluggish uptake over the past three decades. The pace of progress is rapidly accelerating. In the coming 5-10 years, we can anticipate the proliferation of thousands, if not millions, of distinct applications harnessing this technology. We find ourselves at a juncture where the opportune timing allows us to leverage this incredible tool poised to revolutionize the internet.

So hop aboard the bandwagon and begin delving into ZK-proofs.

”



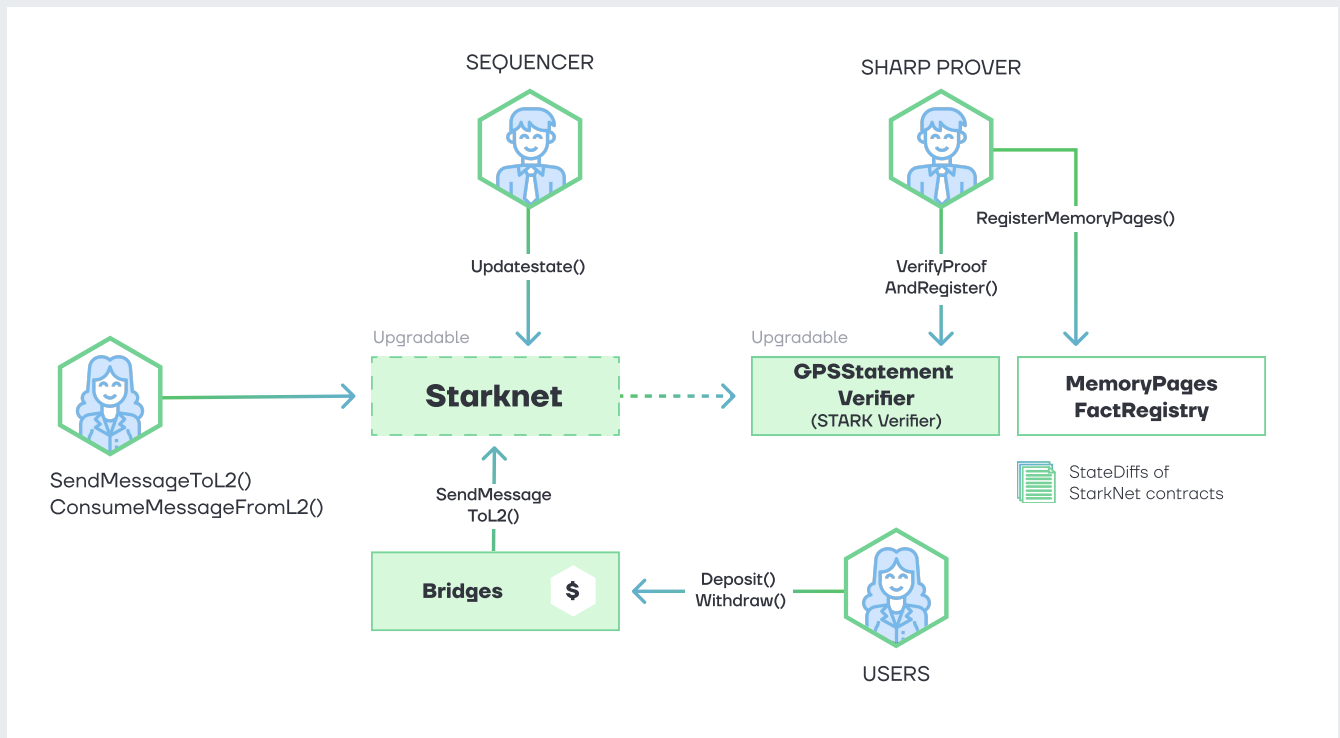


Figure 17: Starknet architecture

Source: L2BEAT

StarkNet runs on ZK-STARK proofs (Scalable, Transparent ARgument of Knowledge) or (STARK Validity Proofs) technology, under development since 2019 by Starkware. Validium allows data to be stored offline, greatly democratizing the price of development.

STARKs are validity proofs that ensure computational integrity using advanced cryptography. They offer polylogarithmic verification complexity and proof size, along with quasilinear proof complexity. Moreover, STARKs rely on minimal assumptions that provide post-quantum security.

SHARP (shared prover) is a service designed for generating proofs that validate the accurate execution of Cairo programs. It is specifically utilized to ensure the correctness of Starknet state transitions, acting as the operating system for Starknet.

- On April 4, 2022, StarkNet launched testnet bridge - StarkGate Alpha. Vitalik Buterin personally reviewed most of the articles published by StarkWare.

StarkNet implements user accounts as smart contracts and uses the native high-performance Cairo language, unlike Ethereum and other EVM-L2. StarkNet transactions are not recorded in a chain; instead, they only state changes resulting from the transactions recorded on L1.

According to Starkware, StarkNet implements a system of recursive proofs, where proofs are generated to reduce the size of the proofs, similar to a Meckle tree. At the same time, Starkware says the verification time is significantly reduced.

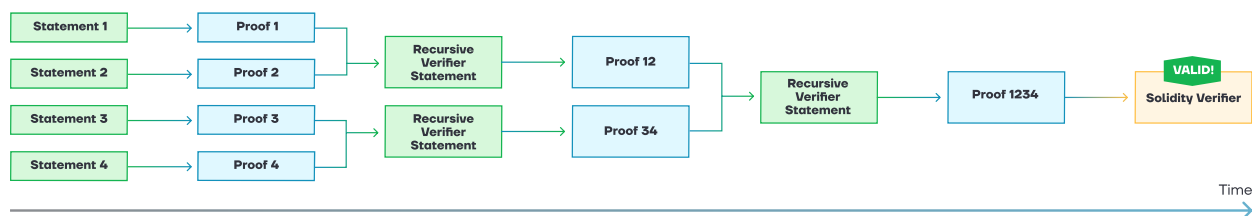


Figure 18: A typical recursive proving flow

Source: Starkware

## ARCHITECTURE:

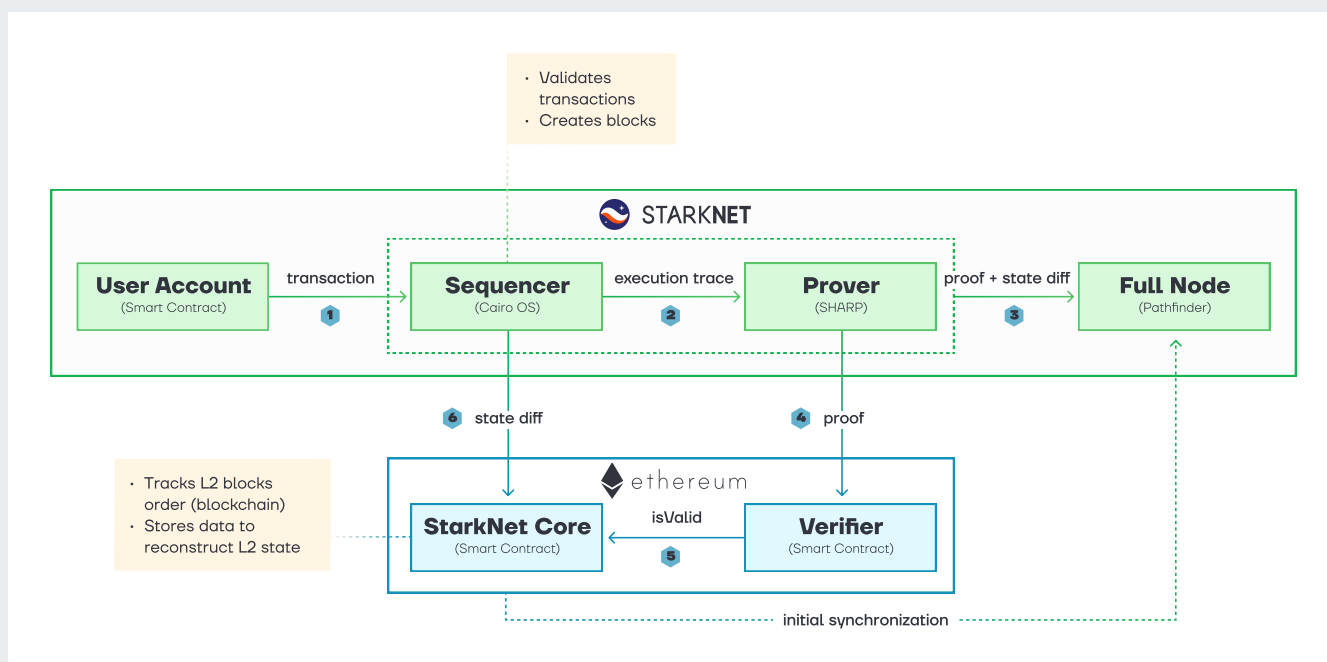


Figure 19: Starknet architecture

Source: StarkNet's Architecture Review, David Barreto

**Full Nodes** (for accounting transactions and storing network backups), Verifier (smart contract on Ethereum, which checks Prover proofs and confirms a state-update validity proof). Sequencer and Prover are currently centralized services, but Permissionless Sequencer and Prover s a development point in the roadmap, suggesting a possible policy change in the future.

- **Sequencer** – an off-chain server that receives all transactions, orders, and checks and joins them into blocks.
- **Prover** (Shared Prover, SHARP) is responsible for creating a cryptographic proof, confirming the integrity of the computation performed by the sequencer when it receives a new global state by executing the transactions contained in the new block). SHARP also allows applications to combine their transaction batches into a single proof, which saves significant commission on L1 proof verification.

- **StarkNet Core contract** receives (validated) state roots from Sequencer, allows users to read L2 -> L1 messages and send L1 -> L2 messages, tracks global L2 state changes from StarkNet every time a new L2 block is created, and its cryptographic proof is successfully verified in L1 Verifier.
- **Gps Statement Verifier** - Starkware SHARP verifier is shared by StarkNet, Sorare, Immutable X and [rhino.fi](#). It gets STARK proofs from the prover, which testify about the integrity of the execution trace of these four programs.
- **Memory Page Fact Registry** - one of the many contracts used by the SHARP verifier. It is important since it logs all the necessary data in the chain, such as the state differences of the StarkNet contracts.

## STAREX

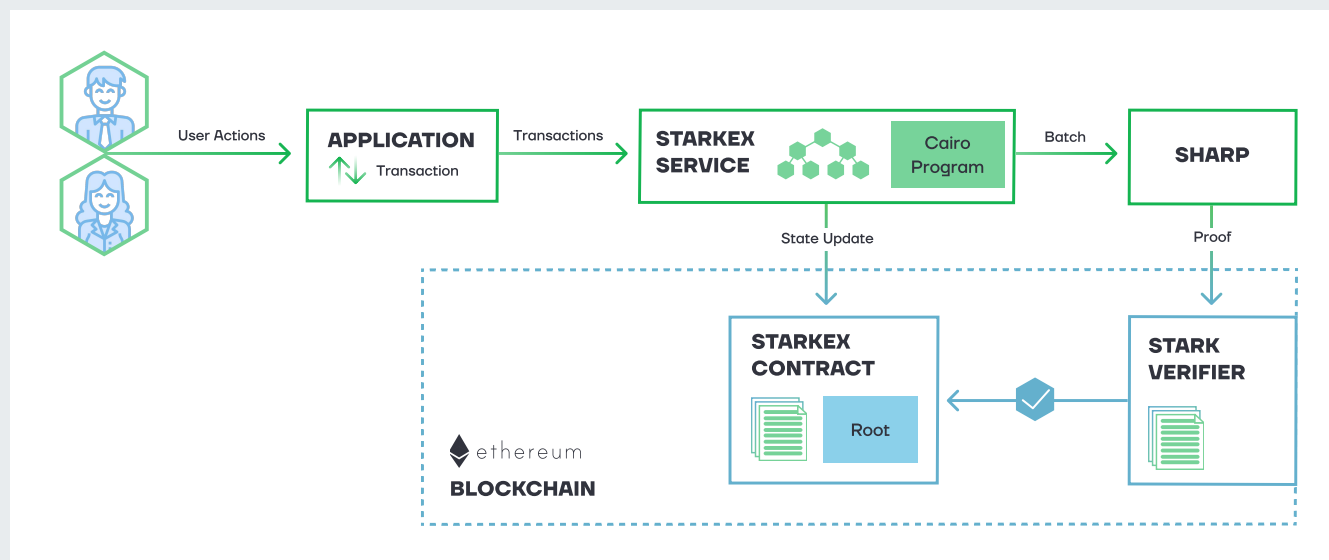


Figure 20: StarEx architecture

Source: Starkware

StarEx has been deployed on Ethereum Mainnet since June 2020 and is a separate area from StarkNet based on validity proofs. It allows you to create something akin to your own rollups for dApps. It's a customizable service that shares the execution of transaction processing and confirmation, performing and validating them offchain.

1. All transactions in the system are executed by the application and sent to the StarkEx Service.
2. The StarkEx Service batches transactions and sends the batch to SHARP, a shared proving service, to generate a proof attesting to the validity of the batch.
3. SHARP sends the STARK proof to the on-chain STARK Verifier for verification.
4. The StarkEx Service then sends an on-chain state update transaction to the StarkEx Contract, which will be accepted only if the verifier finds the proof valid.

The StarkEx system has an off-chain component and an on-chain component:

### The off-chain component:

- Holds the state of orders;
- Executes transactions in the system;
- Sends state updates to the on-chain component.

### The on-chain component:

- Enforces the validity of state transition;
- Holds state commitments and system assets;
- (StarkEx Spot Trading) Manages on-chain accounts, which are useful in the context of Layer 1 (L1) dApp interoperability and DeFi pooling.

StarkEx makes your user's data available using the following data availability modes:

- ZK-Rollup mode.
- Validium mode.
- Volition mode, which enables your user to choose between ZK-Rollup or Validium mode for each transaction.

## LAYER3

StarkNet plans to implement L3; additional layers (L4, etc.) can be built on top of it. Independent L3s will be able to communicate with each other via L2, meaning StarkNet will be able to "hyper-scale."

Applications from StarkEx will be migrated to L3, significantly increasing their scalability and making transaction prices cheaper. Network security will remain commensurate with Ethereum's L1.

L3 can also be used as a canary network similar to Kusama for Polkadot. It will allow protocols and applications to undergo a test period before their release on the main StarkNet network.



**EDUARD JUBANY TUR**  
Founder at ZKX



ZKX is the first perpetual futures DEX on Starknet with self-custody and true community governance.

The popularity of zero-knowledge (zk) tools, particularly ZK-rollups, has grown significantly over the past year as a solution for scaling Ethereum. With improved accessibility to developers, these tools can be leveraged without requiring a deep understanding of complex math and engineering. ZK-rollups offer reduced transaction costs, scalability, and default privacy, making them a relevant solution even after Ethereum's upgrade.

The anticipated launch of zkEVMs is expected to further enhance this trend, with account abstraction driving mass adoption. However, there are still challenges to be addressed in the decentralization of the sequencing and proving systems. Several solutions have emerged, including on-demand sequencing for rollups or on-demand proving of transactions, while account abstraction can potentially address user experience issues in DeFi, bridging across rollups remains a concern.

Nonetheless, the importance of scalable, secure, and privacy-preserving solutions for blockchain networks is growing, as evidenced by the popularity of zk-rollups. They present promising opportunities for the future of DeFi.

Zero-knowledge proofs have become a game-changer in the web3, critical in enhancing blockchains' privacy, scalability, and security. As the competition heats up, we see exciting advancements like StarkWare's Starknet, Polygon's zkEVM, and Matter Lab's zkSync Era, all in the race. The current state is promising, with decreasing hardware costs and the maturing of high-level languages like Noir, Leo, and Cairo. In the future, ZK-rollups will be an integral part of the infrastructure, and people won't have to worry about which one they are using. This competition among ZK players drives innovation, leading to even better and more efficient solutions. While we have a long way to go, the future is bright.

Among investors:



STARKWARE

AMBER



crypto.com



Huobi Global

HASHKEY  
Capital



Orange DAO



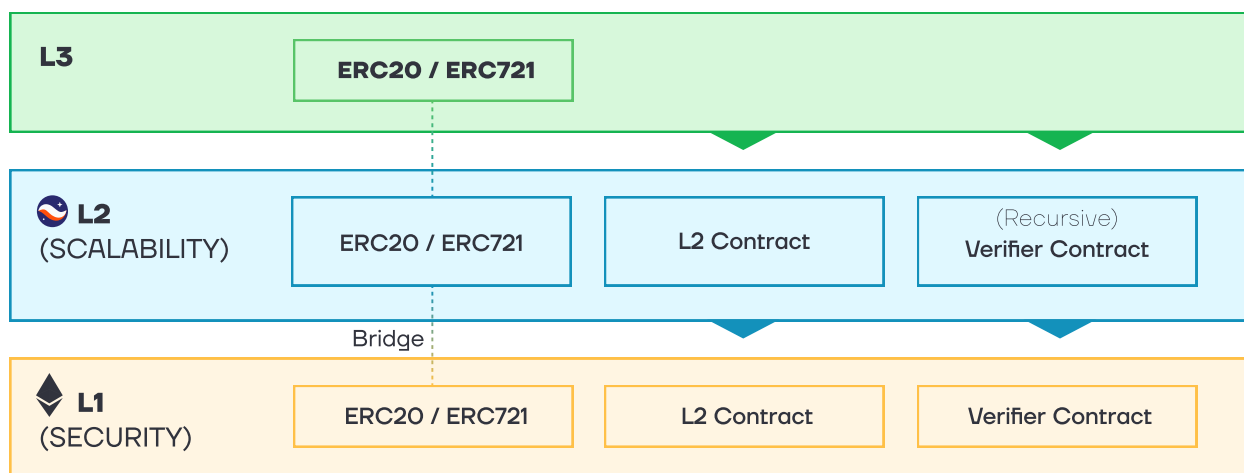


Figure 21: Starknet L3 architecture

Source: Starkware

“



**ETHAN**

R&D Leader of zkPass



zkPass is a composable, privacy-preserving identity protocol based on MPC (Multi-party Computation) and ZKP (Zero-knowledge Proof)

The field of zero-knowledge proofs (ZKPs) is currently experiencing rapid growth, with groundbreaking research and development emerging consistently. Essentially, ZKPs allow for the confirmation of knowledge without revealing the specific details of that knowledge. The applications and use cases for ZKPs span various domains, such as decentralized identity, privacy-preserving transactions, secure and scalable layer-2 rollups, voting systems, ownerships and supply chain verification, among others.

One of the most significant advancements in ZKP research is the introduction of highly efficient and scalable ZKP systems, including PLONK and VOLE-based zero-knowledge protocols. These innovative systems have considerably reduced the computational and storage overhead associated with ZKP generation and verification, making zero-knowledge proofs increasingly practical for real-world applications.

We are convinced that the future of personal data interaction will be significantly influenced by zk-based privacy-preserving identity protocols. By using zero-knowledge proofs (ZKPs), these protocols allow individuals to confirm their identity and share only specific details, without revealing their entire personal information. This approach empowers users to maintain control over their data while enhancing privacy protection.

As our world becomes more interconnected, the need for secure and privacy-focused solutions is growing. ZKPs provide an innovative solution, balancing security and privacy in a way that can be applied across various industries, such as finance, healthcare, education, and e-commerce. The adoption of ZK-based identity protocols can promote trust and collaboration between users and organizations while helping to meet regulatory requirements in areas like data protection and anti-money laundering.

Furthermore, ZK-based identity protocols can act as a bridge between traditional web applications (web2) and decentralized blockchain-based applications (web3), enabling smooth interaction between these different digital ecosystems. As a result, privacy-preserving solutions like these have the potential to drive widespread adoption of decentralized technologies, leading to a new age of secure and privacy-focused digital experiences.

ZKPs are expected to maintain their crucial role in the evolution of secure and privacy-preserving technologies. In particular, they will be integral to privacy-oriented applications in client scenarios, such as those employed by zkPass. As the range of applications and use cases for ZKPs expands, we can anticipate continued progress in ZKP research and development. This progress will likely lead to the creation of even more efficient and scalable systems, ultimately driving the widespread adoption of ZKP technology across various industries.

”



## ECOSYSTEM

Since the mainnet launch in 2020, StarEx technology has been used in DyDx, Immutable, Sorare, Venus Protocol, Myria, Reddio, and Deversifi. Thanks to StarkEx, the listed protocols have had a huge total trade turnover, according to Starknet - \$780 billion and TVL \$500M+. It's also worth noting that StarkNet allows interaction between decentralized applications, while StarkEx does not.

The main projects are DeFi, directives, and games. As of late February, the ecosystem is shown in the image below. It's worth noting that Starkware has very poor EVM compatibility, so there are no EVM-specific protocols like Curve, Aave, or Uniswap.

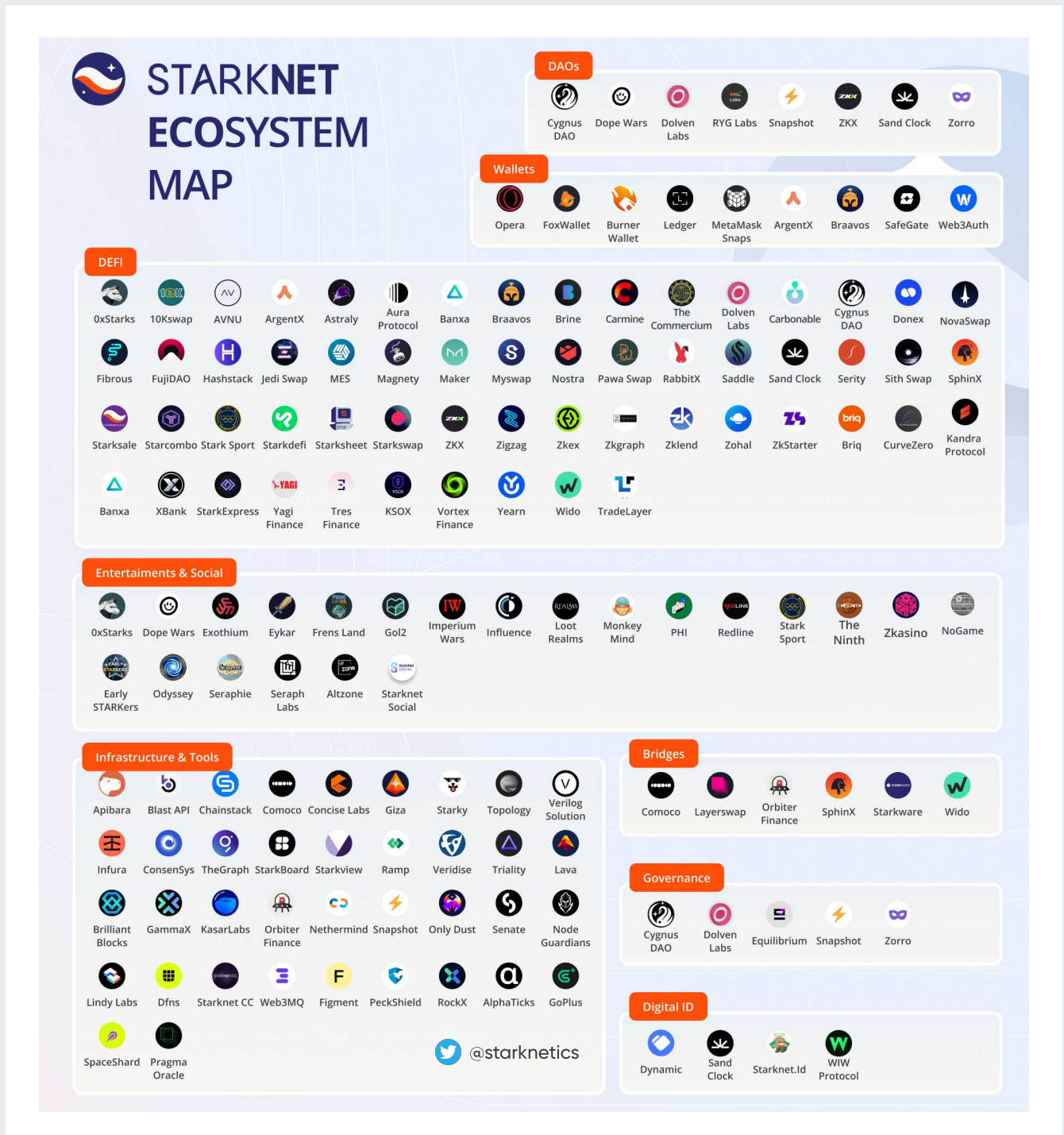


Figure 22: Starknet Ecosystem

Source: Starknetics

## NETWORK AND TVL ACTIVITY:

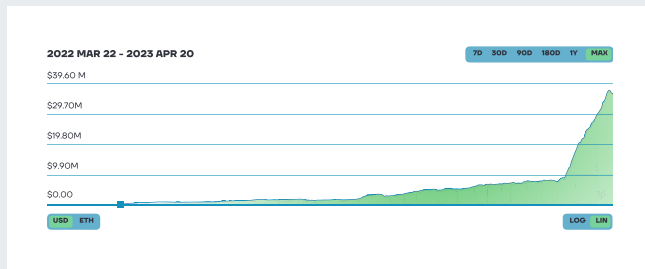


Figure 23: Starknet TVL activity

Source: L2BEAT

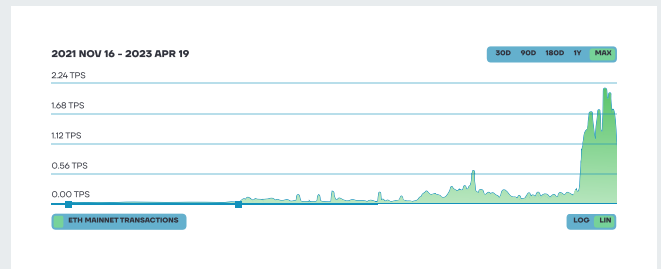


Figure 24: Starknet network activity

Source: L2BEAT

According to Dune Analytics, the volume of funds passed through the StarkNet bridge is lower than that of zkSync. A total of 4,500 ETH (\$7 million at current exchange rates) was deposited to the StarkGate bridge, with the volumes of deposits and withdrawals being similar.

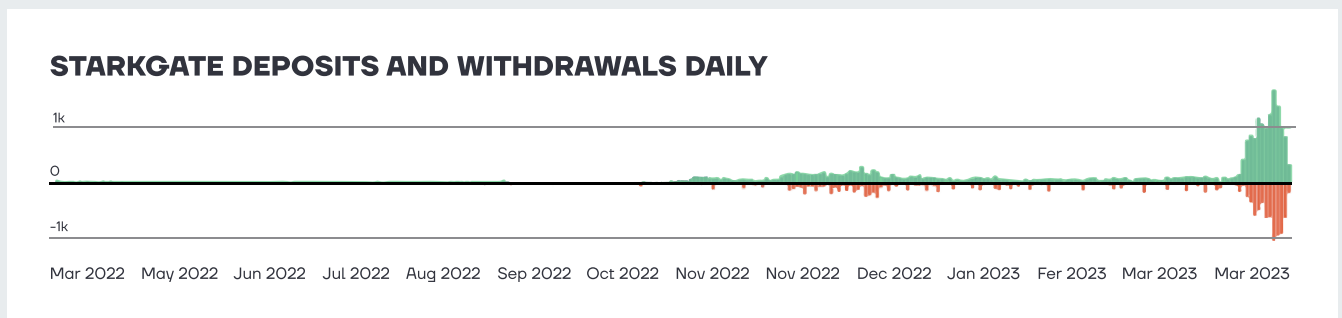


Figure 25: StarkGate deposits and withdrawals daily

Source: Dune Analytics

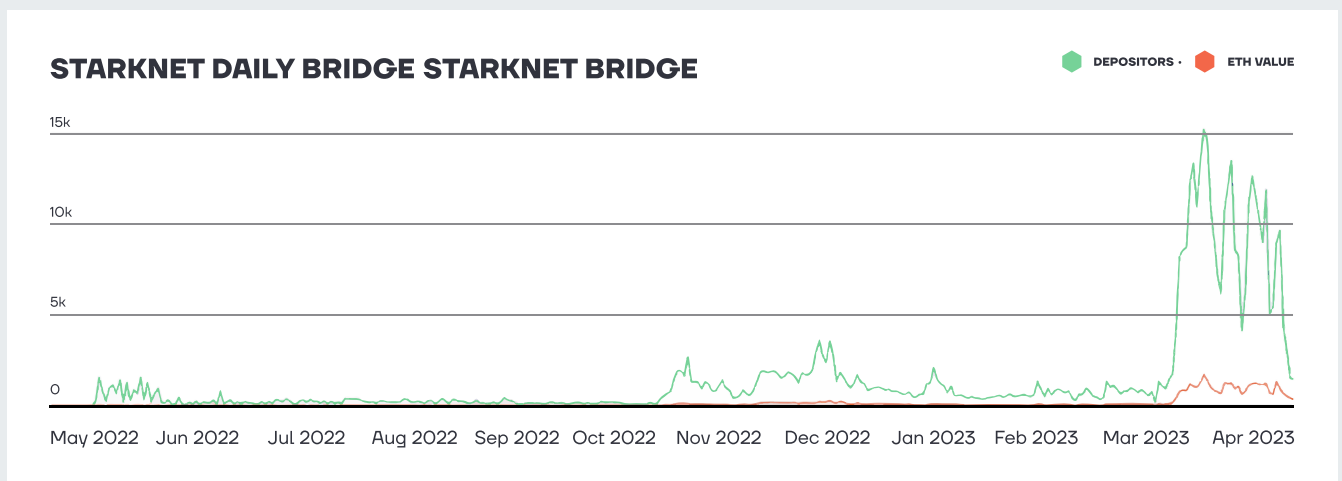


Figure 26: Starknet daily bridge

Source: Dune Analytics

## FUNDRAISING AND INVESTORS

Total raised \$270M+, **Main investors:** Sequoia Capital, Paradigm, Ethereum Foundation, Pantera Capital, Alameda Research, Three Arrows Capital, Founders Fund and others.

**Major Infrastructure Partnerships:** Consensys, Nethermind, OpenZeppelin, Infura, Ledger, Alchemy, Arcane Assets, OSS Capital. Also, Visa recently said they want to try Starknet for transactions.

### III. SCROLL



Scroll is a cutting-edge ZK-SNARK rollup designed to leverage EVM compatibility, ensuring seamless migration for existing applications from L1. Collaborating closely with the Ethereum Foundation, Scroll actively works on zkEVM virtual machine and gets positive feedback from influential figures, such as founder Vitalik Buterin. The project has also established a strong presence within the Asian Ethereum community, particularly in Vietnam.

It has allowed the creation of Ethereum smart contracts, establishing Scroll as an EVM compatibility type 2 ZK-rollup. The backbone of Scroll's robust cryptographic framework is a modified version of Halo 2, a Plonk-based verification system developed and maintained by the Zcash team.

To enhance the speed of proof computation, this project is actively exploring the utilization of FPGA or ASIC graphics processors, promising exciting possibilities for performance optimization. Scroll also creates a sophisticated rollup architecture that promotes parallelization and pipeline computing.

Since February 2023, Scroll has transitioned from the Pre-Alpha testnet - which lasted for six months - to the Alpha testnet on the Goerli network.



**SHAHRYAR HASNANI**

Partnerships at  
Scroll

#### **Scroll and Ethereum Build the Future of ZK and Blockchain Together**

Scroll has been built on the vision that a blockchain's longevity is upheld by its core values, legitimacy, and culture—and as a scaling solution building towards Ethereum's endgame, we should strive towards their values and culture of decentralization and credible neutrality.

For the past two years, we've been building an open-source, bytecode-compatible zkEVM in close collaboration with the Ethereum Foundation's Privacy and Scaling Explorations group. We have actually contributed to about half of the PSE's zkEVM codebase (and vice versa), meaning we're not just Ethereum-aligned—we're directly supporting the development of Ethereum's future.



**Scroll**

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

Scroll's focus on these values is evident in our technical excellence and entire architecture: we've pushed for bytecode-compatibility, we're supporting Ethereum's standard execution trace with minor modifications, and we have modeled our sequencer off of Geth. This has resulted in substantially fewer infrastructure vulnerabilities and a seamless developer / user experience that many consider to be best-in-class and nearly identical to that of Ethereum. That means fewer concerns around re-audits and, for many developers, the process of porting over projects and dApps takes only a matter of minutes.

Scroll has been on Alpha (Goerli) testnet since the end of February, and has had significant traction with over 38M transactions, 7M wallet addresses, 2.7M contracts deployed, and an average of ~250K transactions per day. We plan on launching on Sepolia testnet in a month and aim to launch on mainnet in Q3; and we're not stopping there. Decentralization of both our provers and sequencers is a priority for Scroll, and extensive research is underway to ensure the security, stability, and success of the network—and by extension, the Ethereum ecosystem itself.

## ARCHITECTURE

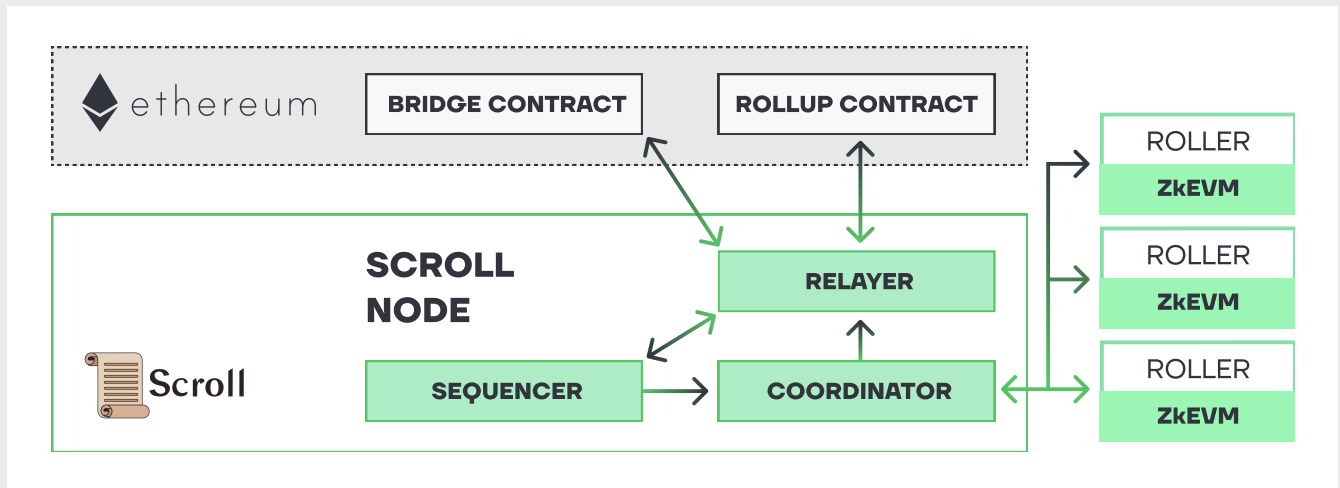


Figure 27: Scroll architecture

Source: Scroll

1. Scroll Node is a key component of the Scroll architecture. By creating L2 blocks with user transactions, it commits them to the Ethereum main network, therefore reducing communication between L1 and L2.

- Every few seconds, Sequencer generates L2 blocks and updates the state root. Once a new block is generated, it sends an execution trace to Coordinator.
- Coordinator receives the execution trace and sends it to a randomly-selected Roller for further validity proof generation. Every N blocks, the Coordinator sends validity proof batches to a Roller, that then aggregates them into a single block proof. Afterward, Coordinator sends the aggregate proof to the Rollup contract that finalizes L2 blocks.
- Relayer monitors the messages about deposits and withdrawals on L1 and L2 Bridge contracts. It also tracks the L2 blocks' state and validity proofs to provide actual data availability.

2. Roller Network:

- Roller creates validity proof for execution trace and sends it back to the Coordinator. Sometimes Rollers have to combine proofs from multi-zkEVM circuits into a single-block proof.
- To make proof generation faster, multiple Rollers can work in parallel to generate proofs for different blocks simultaneously.
- Also, Rollers Generates zkEVM validity proofs using GPUs, FPGAs, and ASICs to reduce the proving time and associated costs.

3. Rollup and Bridge Contracts: Ensure data availability, validate zkEVM proofs, and enable asset transfers between Ethereum and Scroll.

- Rollup contract provides L1 security level and data availability for Scroll L2 blocks. It verifies the aggregate proofs against previously submitted L2 state roots and blocks. After this procedure, it stores state roots on-chain and L2 block data as Ethereum calldata, and this way, blocks become confirmed.
- Bridge contracts communicate between L1 and L2 through messages controlling the bidirectional bridging of ERC-20 assets.

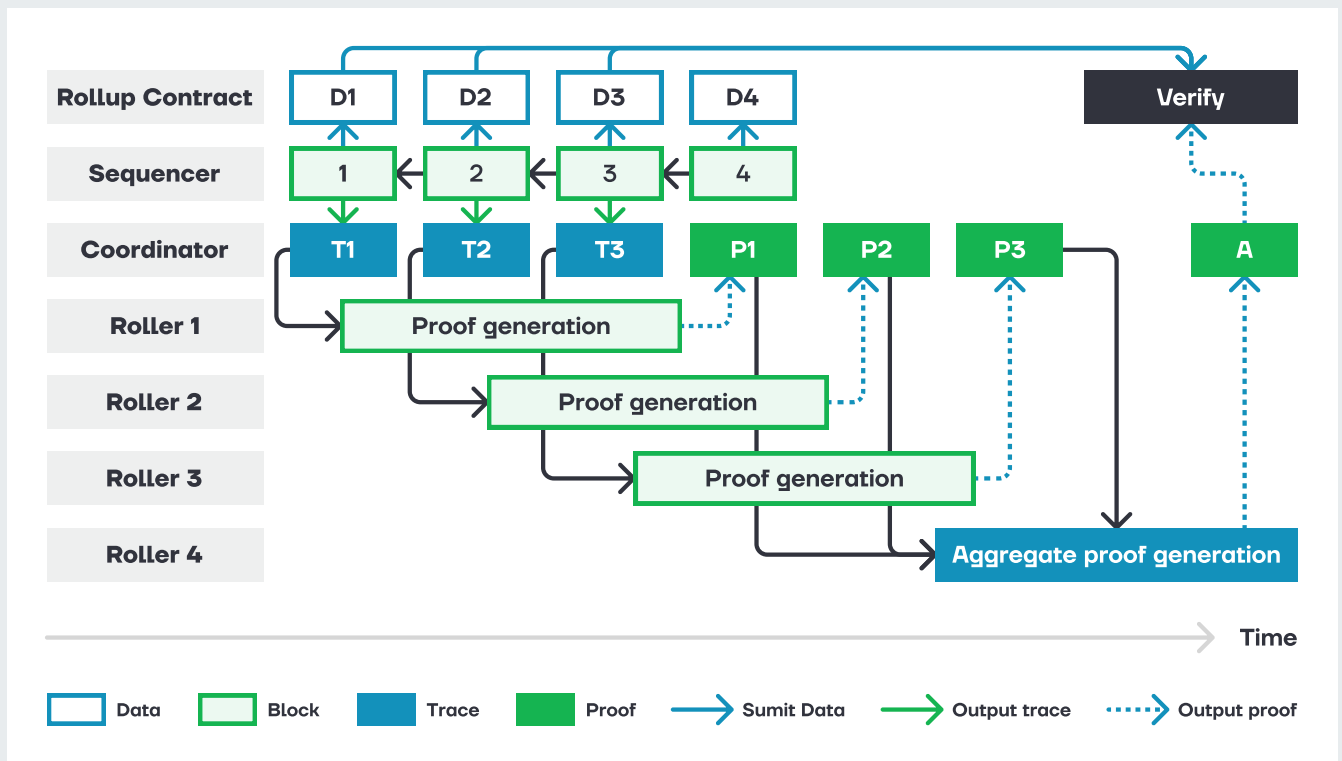


Figure 28: Scroll workflow  
Source: Scroll

Roller Network is a decentralized Provers network that generates validity proofs for every new Scroll L2 block. Firstly, Roller converts the execution trace received from the Coordinator into circuit witnesses. Next, it produces proofs for each zkEVM circuit. Finally, proof aggregation combines the proofs from multiple zkEVM circuits into a single, comprehensive block proof.

Scroll zkEVM is a mechanism that utilizes succinct ZK proofs to validate the accurate execution of native EVM bytecode. This innovative approach offers robust guarantees on the EVM's state transition function, enabling Scroll to support Ethereum native developer tooling, including the JSON-RPC interface and transaction format.

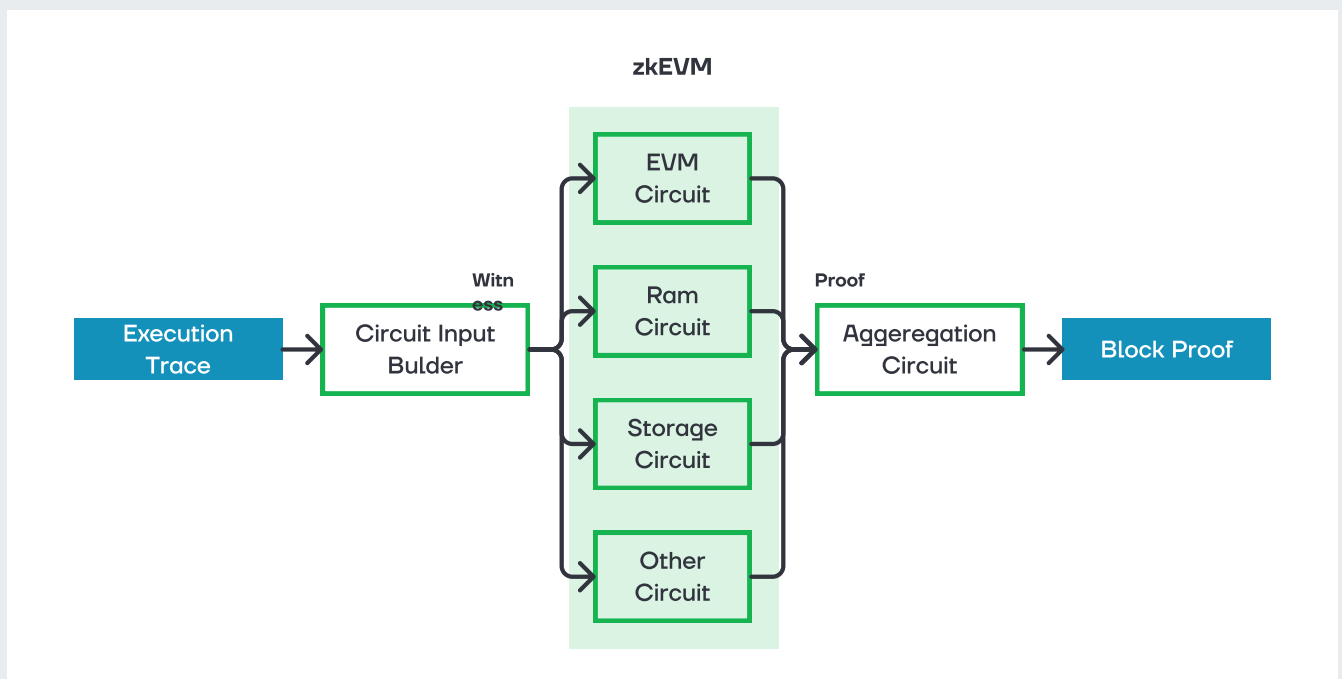


Figure 29: Roller workflow  
Source: Scroll



## INVESTORS

Scroll raised in total \$80M+ with current \$1.8B valuation. In April 2022, this new crypto-unicorn closed Series A with Polychain Capital, Bain Capital Crypto, Robot Ventures, and several Ethereum Foundation members. In 2023 there was a new Funding round with \$30M from Sequoia Capital China, Polychain Capital, Variant, and others.

## ECOSYSTEM

As Scroll leverages EVM compatibility, it ensures consistent migration for existing applications within the Layer1 Ecosystem. Projects face no issues expanding their influence within the blockchain by transitioning to Scroll, as they can also be expanded to any other EVM-compatible network.

Ever since the Scroll Team announced the Alpha Testnet on the Goerli Network, the entire Scroll Ecosystem has witnessed substantial growth, with around 127 projects now in the process of expansion or relocation, and soon to be launched on Scroll.

Most of the projects that will be launched on Scroll are related to the creation of infrastructure around the Ecosystem so far, which creates excellent conditions to provide an opportunity for extensive testing and refinement before its full launch later on.

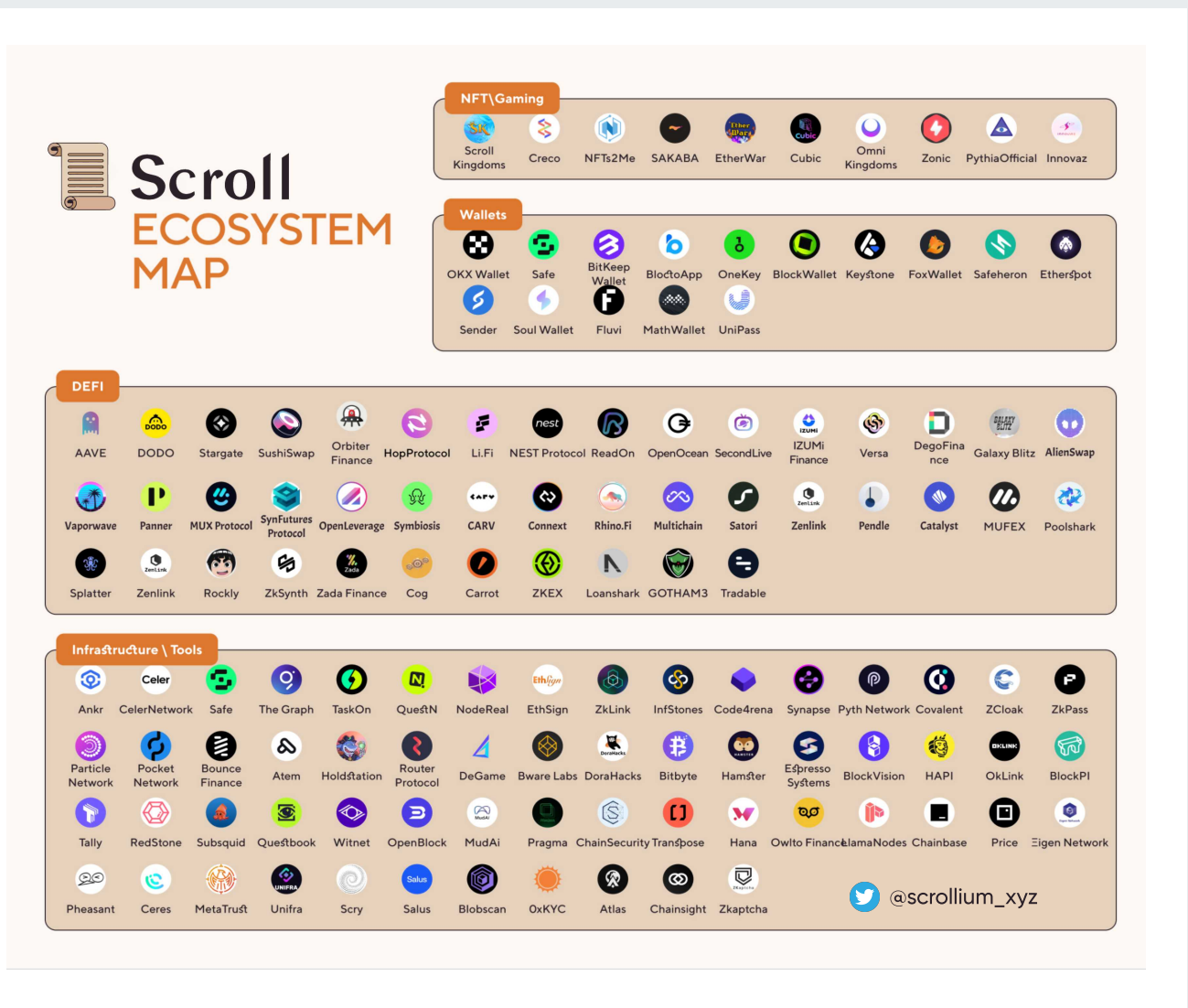


Figure 30: Scroll Ecosystem Map

Source: Scrollium

## IV. INTMAX

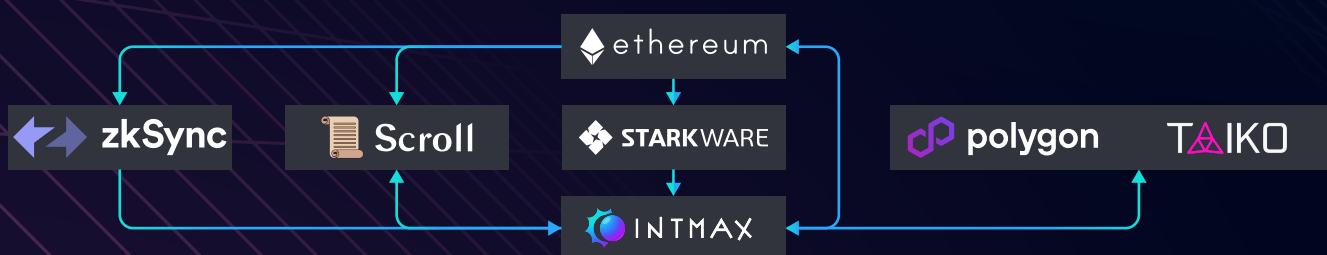


Intmax, as a stateless layer of Ethereum, will have a unique role in this space, not competing with the other stateful Layer2s. The majority of the value of Ethereum, in comparison with Bitcoin, is the statefulness. This statefulness allows for the utilization of DeFi, for example. However, users of Ethereum also demand an interoperable stateless payment/NFT layer to support simple usages and to support all of these stateful L1/L2. This is similar to UDP of the TCP/IP.

Intmax plays a different role from the existing scaling solutions, and this is the missing part of Ethereum.

Building the stateless architecture of Intmax is a powerful way to have these features: near-zero gas cost and privacy, at the same time. Stateless means that block producers (validators) and the client side don't have databases, unlike the usual ZK-rollups. We can shift the computation cost and the data availability cost to the client side. Then, validators and blockchain nodes need not know and do almost anything. Anyone can be a block producer since it's cost-free. Therefore, we can have an unstoppable network that has both hyperscaling and privacy.

	INTMAX	STATEFUL ZK-ROLLUPS	LIGHTNING NETWORK RGB
State	Stateless	Stateful	Stateless
On-Chain cost (fee)	Extremely Low	Low	Extremely Low
Confidentiality	High	No	High
Node for users	Not Required	Not Required	Always Required
Smart contract	Interoperable	Complete	P2P
Client side zkp	Required (3-5 sec)	No	No
Finality	L2 Block	L2 Block	Instant
Stateful defi	No	Yes	No
Censorship	Difficult	Easy	Difficult
Parallelization	Unlimited	Very Limited	Unlimited
Interoperability	No	No	No



“

The vision of Intmax is to make Ethereum a globalized property system that can accommodate all kinds of online citizens. Ethereum and the Internet should be the largest supporter of property rights, even in places where legal systems are not trustworthy. To achieve this goal, the fee should be near-zero for any kind of person, and privacy should be solid to avoid people being targeted by crimes.

”

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

In April 2023, Intmax raised \$5M in seed funding from investors like Cryptomeria Capital, Hashkey Capital, Bitscale Capital, Scroll, and others.



**LEONA HIOKI**

Co-founder of INTMAX



## V. AZTEC NETWORK



Aztec Network is a private ZK-rollup on Ethereum, allowing applications to access privacy and scale. There are some similarities to Bulletproofs, as Aztec also uses range proofs. Aztec Network was founded in 2017 as an institutional platform Creditmint. In 2019, it introduced PLONK, launched the ZK in 2021, and Aztec Connect in 2022.

The first attempt at online privacy with ZK-rollup was Aztec 1. Aztec 1 was slow, inefficient, expensive and limited in its functionality to basic private transactions.

The next work was a set of infrastructure and privacy tools for Ethereum called Aztec Connect. Not only did it extend the privacy functionality in Ethereum beyond simple payments and interaction with arbitrary smart contracts, but it hinted at the cost savings that could ultimately be achieved by encrypted storage packets through packet-based transaction processing.

Aztec Connect was an important step in the mission to create a fully programmable encrypted ZK-rollup. Not only did it provide critical feedback, but it also proved the compatibility of contracts for sequencer and hoarding packages. The tremendous effort and research invested in Aztec Connect led the team to develop Aztec 3, the next-generation Aztec protocol.

### ARCHITECTURE

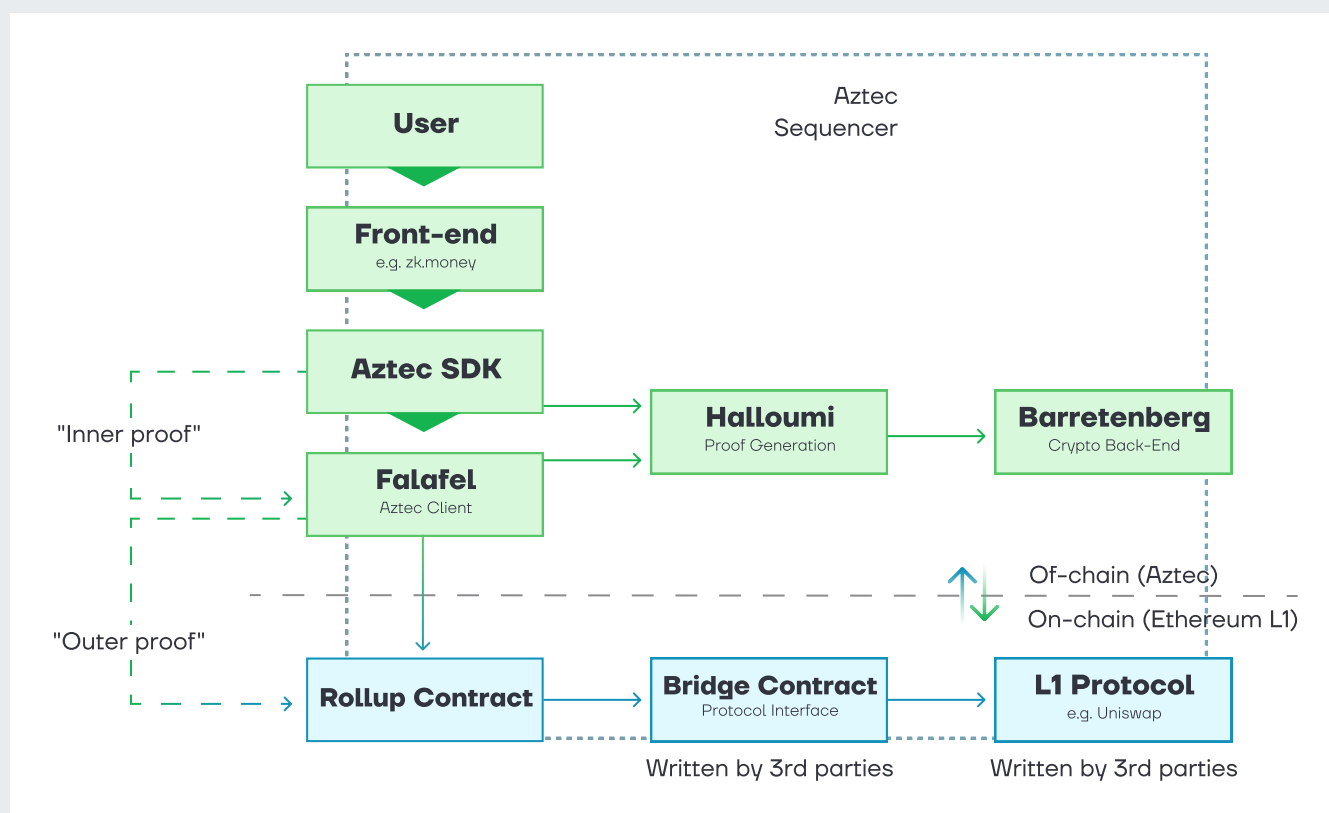


Figure 31: Aztec architecture

Source: Explaining the "Network" in Aztec Network, Jon Wu

Aztec rollup is protected by the industry-standard PLONK verification mechanism and uses ZK-SNARK evidence. In addition, Aztec allows users to access their applications at Level 1 confidentially.

Accounts have a single public key for access and two private keys, one for viewing balances and one for fund transfers. Both keys can be used on different devices.

- **Aztec SDK** manages sensitive information without transferring it to a third party and accepts and decrypts data for the developer's use. The SDK updates the state and sends the proof to the Aztec sequencer.
- **Sequencer** is used only to aggregate proofs. It does not perform calculations.
- **Falafel** is responsible for the client side. The software takes the proofs from the client, aggregates them, and sends them for checking. This is the batching mechanism for the end user. Anyone can run the Falafel client and become a sequencer.
- **Aztec Connect SDK** is a platform to simplify the integration of DeFi ecosystem projects.
- **Zk.money** is privacy-centric farming aggregator.
- **Noir** is a language with simplified syntax for writing encrypted applications (not yet launched). With Noir, developers can develop using familiar Rust-based syntax, making ZK applications more readable, secure and easy to understand.

## SEVERAL SMART CONTRACTS DRIVE THE SYSTEM

- **RollupProcessor**. The main rollup contract is responsible for deposits, withdrawals, and receiving transaction packets along with ZK-proof. The following tokens are stored in this contract: ETH, DAI, renBTC, and USDT.
- **TurboVerifier**. Turbo Plonk ZK-SNARK verifier. The owner can upgrade it without delay.
- **AztecFeeDistributor**. The contract is responsible for distributing commissions and reimbursing gas to aggregate suppliers.

## ECOSYSTEM

Ecosystem Aztec Connect includes Aave, Curve, Lido, Element, Set Protocol, Compound and Liquity. In addition, Aztec Grant-funded independent companies: [Nucleo](#), [Trelis](#) and [zkGiving](#), are working on their applications.

## ACTIVITY ON THE WEB AND TVL

It is also worth considering that Aztec announced in mid-March 2023 that they are discontinuing support for Aztec Connect and are focusing on further developing their brainchild to further develop a truly decentralized, universal encrypted ZK-rollup with Ethereum security.

## INVESTORS

It recently closed Series B \$100M with investors in a16z, A Capital, King River, Variant, SV Angel, Hash Key, Fenbushi, and AVG.

In December 2021, raised \$17M in Series A from Paradigm, a\_capital, Ethereum Ventures and Libertus Capital, Variant Fund, Nascent, IMToken, Scalar Capital, Defi Alliance, IOSG Ventures, and ZK Validator, as well as Anthony Sassano, Stani Kulechov, Bankless, Defi Dad, Mariano Conti, and Vitalik Buterin.

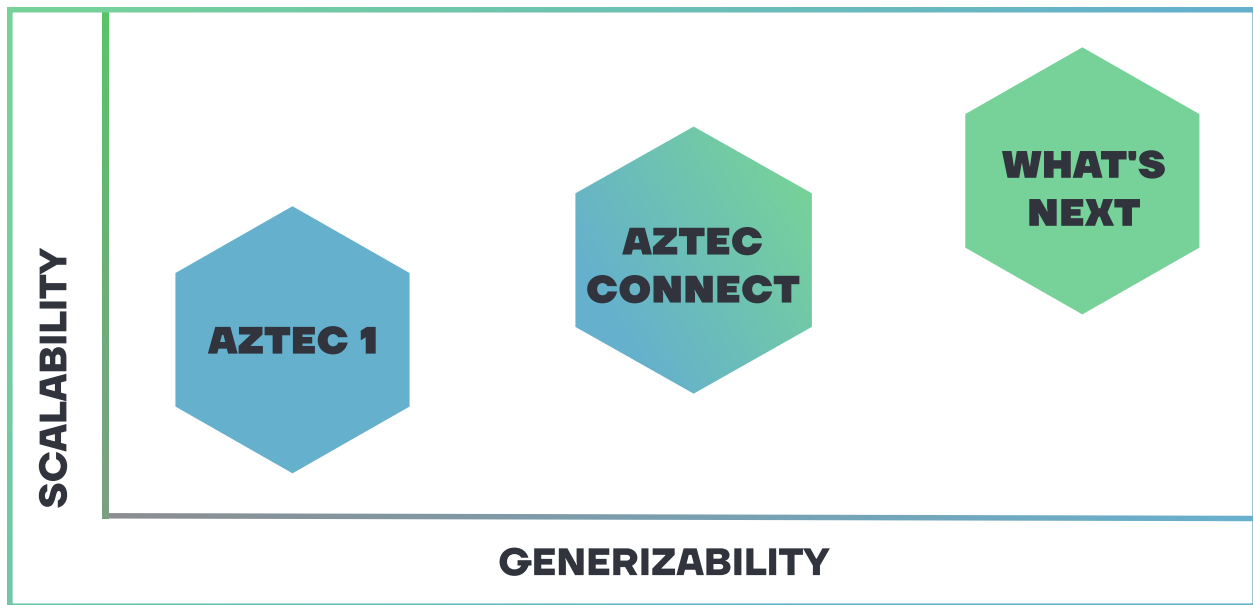


Figure 32: Aztec development

Source: Aztec Medium

“



**EDI SINOŠČIĆ**

Founder & CEO of  
SpaceShard

 **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.

There is a lot of buzz around ZK. Multiple solutions claim to be running their mainnet environments, and it seems ZK summer is just around the corner. However, upon closer inspection, we find that most of these networks have implemented most of the basic features but are still not fully production-ready.

Currently, we have a diverse range of solutions, both on the zkEVM and zkVM side. Validium-like solutions are the main contenders for scaling Ethereum in the short term, with other solutions like Volition and similar ones expected to emerge in the future. There is also an interesting development in privacy protocols like Aztec or Aleph Zero, which promise a future of blockchain that is both scalable and private. While the promise of privacy is still a bit further in terms of maturity, significant developments have already taken place, and we should not underestimate the speed at which they can reach maturity.

When we consider the current status of blockchains, we are far from mass adoption in terms of scalability and user experience. We face expensive transactions and clunky user experiences. Now, the promise of zk solutions is that they will address these issues. Native account abstraction will undoubtedly help, and the scalability of L2s and L3s will reduce fees. Are we on the path to achieving a web2-like user experience? And how far are we from it? Well, five years ago, ZK seemed impossible, but now it is already in production. Similarly, with user experience, it may take time, but it will come as a surprise and will be obvious in retrospect how the whole thing was just around the corner.

But what new use cases can we expect? Currently, we only have DeFi and NFTs as some of the use cases that have gained more traction. In the future, we can expect much more, such as games, autonomous worlds on-chain, and network states, experiments like Zuzalu.

Additionally, there will be many privacy-preserving use cases that will help evolve DeFi as we know it today to a new level.

All in all, we are still in the early adopters' phase of ZK tech. We are discussing whether my idea of the electric supercar is better than yours while still driving an old Mercedes from the 90s. While the Mercedes is still functioning, we are aware that we need a radical change, and the suite of ZK technologies promises to not only make things cheaper and faster but also enable us to communicate and coordinate better, bringing us closer to overcoming the challenges of coordination failure

”



The Polygon zkEVM Mainnet Beta was launched in March 2023. However, the foundation of the Polygon ZK ecosystem can be traced back to 2021 with the inception of the \$1 billion strategic fund, which primarily concentrated on zero-knowledge rollup research. This program was established with well defined objectives:

- Acquiring exceptional ZK projects and assembling talented teams.
- Designing and developing innovative ZK-based solutions.
- Attracting top experts in the field to join the program.
- Providing financial support for research, partnerships, and other related activities.

As a result, several ZK solutions are being developed within the ecosystem, including Polygon zkEVM, Polygon Miden, and Polygon Zero. These products are being created by collaboration between employing different technology stacks and innovations.

“



**GRACE TORRELLAS**

VP Product  
Polygon zkEVM



Polygon zkEVM is the first zero knowledge scaling solution compatible with the Ethereum Virtual Machine to integrate smart contracts and developer tools.

### **Acceleration of Zero-Knowledge Proofs by Polygon Labs Sets the Stage for Blockchain Revolution**

Polygon Labs has helped accelerate the efforts in the field of zero-knowledge proofs (ZK) since 2021. These efforts aim to advance the applications of ZK in blockchain scaling and privacy.

By assembling a team of brilliant minds, researchers, and developers, Polygon Labs has fostered an environment of unparalleled innovation. When the decision was made to construct Polygon zkEVM, many experts in the crypto community predicted it would require a decade to complete. However, here we are in 2023, witnessing the successful deployment of a secure and high-performing Polygon zkEVM mainnet beta.

This remarkable progress is a testament to the collaborative efforts of exceptionally talented individuals. The Polygon Zero team contributed Plonky2, a superfast ZK proving system, while the Polygon Miden team brought their expertise in STARKs to realize recursive proving in Polygon zkEVM. Combining all the efforts, the Polygon Hermez team pioneered the opcode-level compatible zkEVM, leveraging tools and languages like PIL and Circom. Notably, Jordi Baylina, co-founder & technical lead at Polygon zkEVM, developed Circom, a language for programming ZK circuits, which has now become an industry standard.

Polygon Labs researchers' ability to deliver secure zk products ahead of schedule exemplifies their proficiency. Presently, Polygon Labs is making several proposals with a vision for Polygon 2.0, aiming to transform the legacy Polygon PoS chain into a layer-2 validium with ZK-proofs. Ultimately, Polygon Labs intends to see unified liquidity across all Polygon chains using a ZK bridge.

In summary, Polygon Labs has made significant contributions to zero-knowledge technology through open-source and code-available projects. With the rollout of the Polygon 2.0 roadmap, Polygon Labs is undeniably poised to help revolutionize blockchain technology with ZK.

”

Polygon Hermez emerged as a ZK-STARK and ZK-SNARK-based solution, claiming to be the first decentralized ZK-Rollup on the Ethereum network. It positioned itself as the initial implementation of the Ethereum zkASM virtual machine (zkEVM). However, it should be noted that other projects, such as Scroll, were already working on their own zkEVM implementations during that period. Therefore, Hermez was not the sole player in this field.

To address the challenge of ensuring sufficient computational power for ZK generation, a consensus algorithm called Proof of Efficiency (PoE) was proposed. PoE aimed to establish that not every validator with a stake could guarantee, having enough power to generate ZK-proofs effectively.

Polygon zkEVM leverages the entire technology stack of Polygon Hermez and EVM compatibility with ZK storage packages. This integration is a crucial aspect of Polygon's product suite, positioning zkEVM as a high EVM-compatible solution. Some ZKR, such as zkSync, introduced zero-knowledge EVM implementations, while other rollups are currently incompatible with Ethereum (excluding Scroll, which does not yet have a developed ecosystem at the time of this review). This provides Polygon zkEVM with a promising advantage to kickstart its adoption.

Among the projects discussed earlier, Polygon zkEVM boasts the most intricate architecture and transaction lifecycle organization. According to the documentation, zkEVM is the first implementation to incorporate recursive STARK technology. As previously mentioned, zkEVM builds upon Hermez and thus supports both ZK-SNARK and ZK-STARK. Another interesting thing is zkProver which offers a STARK-proof builder and a SNARK-proof builder at the same time. Now Polygon zkEVM architecture is working on the Ethereum Mainnet and Goerli Testnet.



Figure 33: Polygon zkEVM Ecosystem Map

Source: Poly ZK gone

## ARCHITECTURE

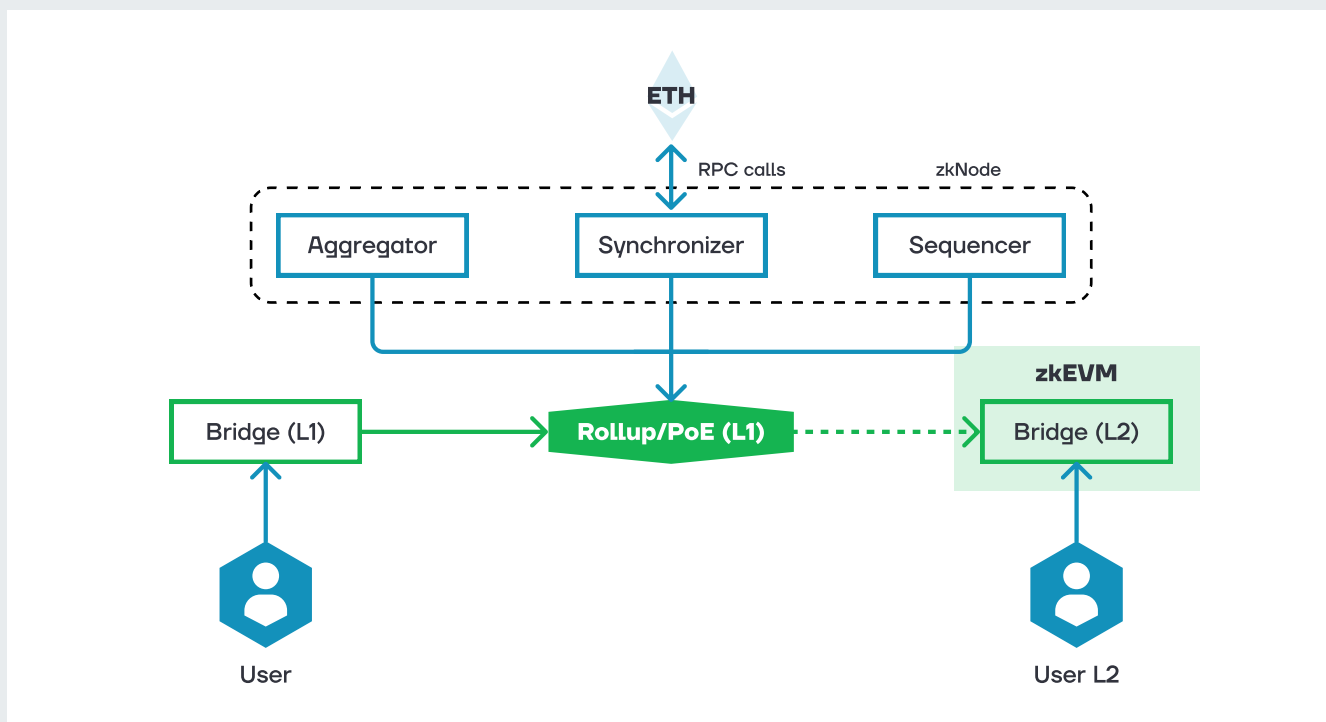


Figure 34: zkEVM Architecture

Source: Polygon zkEVM Documentation

## POLYGON ZKEVM ARCHITECTURE COMPONENTS

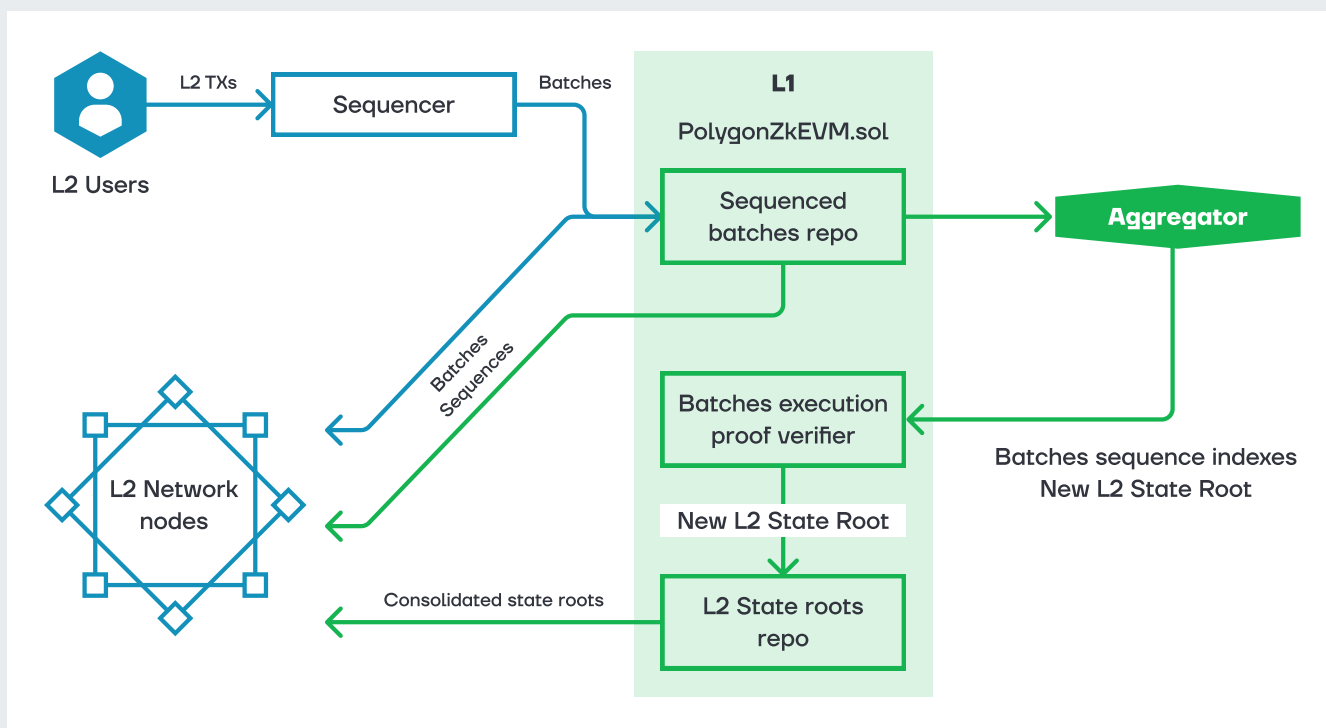


Figure 35: zkEVM Logic

Source: Polygon zkEVM Documentation

- **Consensus Contract (PolygonZkEVM.sol, deployed on L1)** – current consensus version combines decentralized automated Proof of Donation (PoD) auctions (Polygon Hermez 1.0) with participation of multiple coordinators to produce rolled-up transactions from L1 to L2 batches. A ZK-rollup requires on-chain data while ZK-SNARK proofs for transaction validation with further analyses of Prover's final statements.
- **Verifier** – a smart contract that verifies any ZK-SNARK cryptographic proof for every transaction in the batch. It verifies the correctness of a proof, ensuring a valid state transition.
- **zkNode:**
  - **RPC mode** – implements the synchronization to know the L2 state. It updates network data from Sequencer's batches broadcast and verifies by Consensus Contract validated info. It interacts with L1 and synchronizes the local L2 State every two seconds.
  - **Sequencers** – node mode runners that roll up transaction requests into batches and add them to the Consensus Contract. Sequencers earn MATIC fees for completed valid batches and pay some fees for Aggregators to create and propose batches.
  - **Aggregators** – nodes that validate transaction batches and generate validity proofs. They receive all the transaction data from the Sequencer and submit validity proofs for state transition computation. After all computations, Aggregators send Prover's outputs to PolygonZkEVM.sol, which checks ZK-proofs correctness.
    - **zkProver** – key aggregator's component that helps to validate batches and generate validity proofs. It provides ZK-proofs based on Aggregator's transaction info after complex polynomial computations. zkProver comprises several components, including a Main State Machine Executor, multiple secondary State Machines (each with its own executor), a STARK-proof builder, and a SNARK-proof builder.
  - Also, in the non-recursive case, zkProver can work with STARK proofs and integrate them in the initial zkEVM SNARK validation scheme. Prover's State Machine final states are expressed in PIL-Language that can transform into verifiable STARK proofs by using PIL-STARK. Rapid SNARK generates a SNARK proof based on the previous STARK proof and publishes it as the validity proof of the original computation.

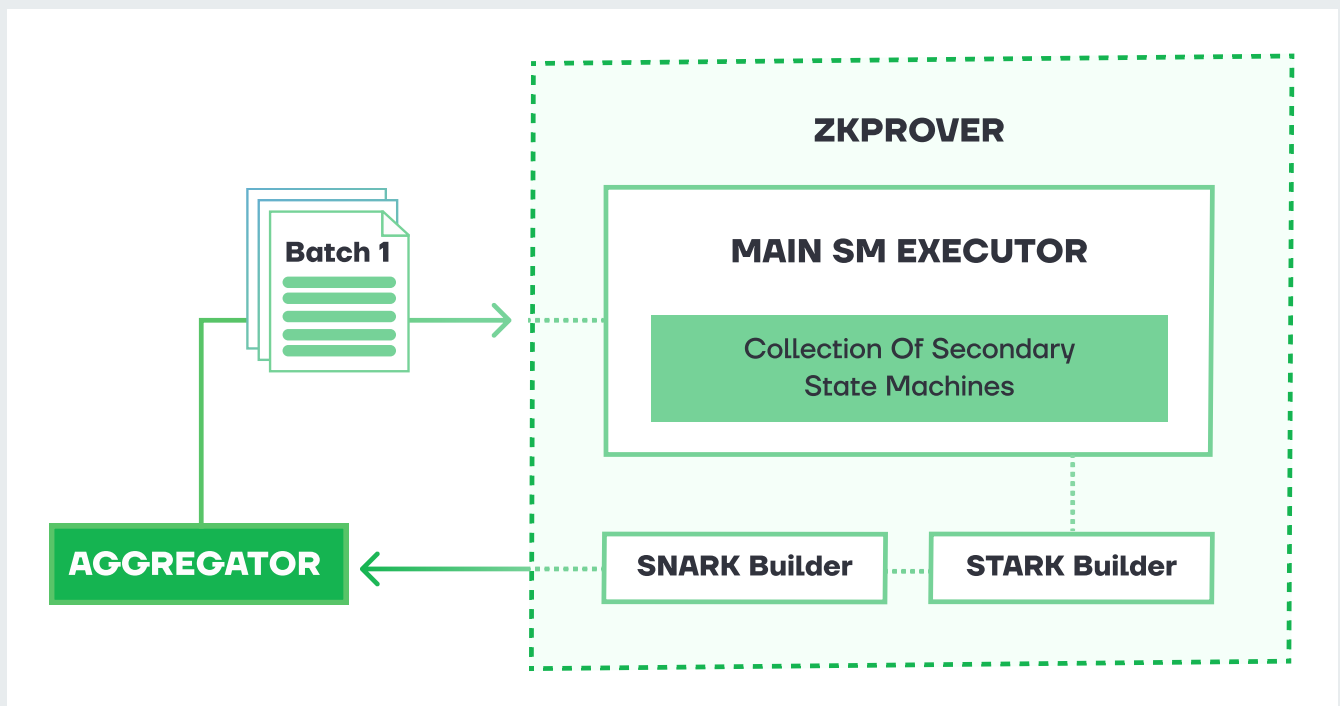


Figure 36: zkProver

Source: Polygon zkEVM documentation

- **zkEVM Bridge** – Smart Contracts for L1 <—> L2 deposits and withdrawals and transactions between different L2 networks. This solution provides data availability for every L1 or L2 nodes for the validation procedure. It utilizes specially designed Merkle Trees that can work with less expensive Keccak hash functions (cheaper fees), generate wrapped tokens the first time a new token is added to the zkEVM network (may be faster), and add more detailed token metadata in the Merkle Trees leaves to protect every transfer.

## ECOSYSTEM

The Polygon zkEVM ecosystem is still in its nascent stage, but it is reported that projects like Lens, Balancer, QuickSwap, Uniswap, Aave, Covalent HQ game projects Midnight Society and Oath of Peak as well as infrastructure providers like ANKR , Alchemy , Sequence and The Graph are launching in the Mainnet beta.

## ONLINE ACTIVITY AND TVL

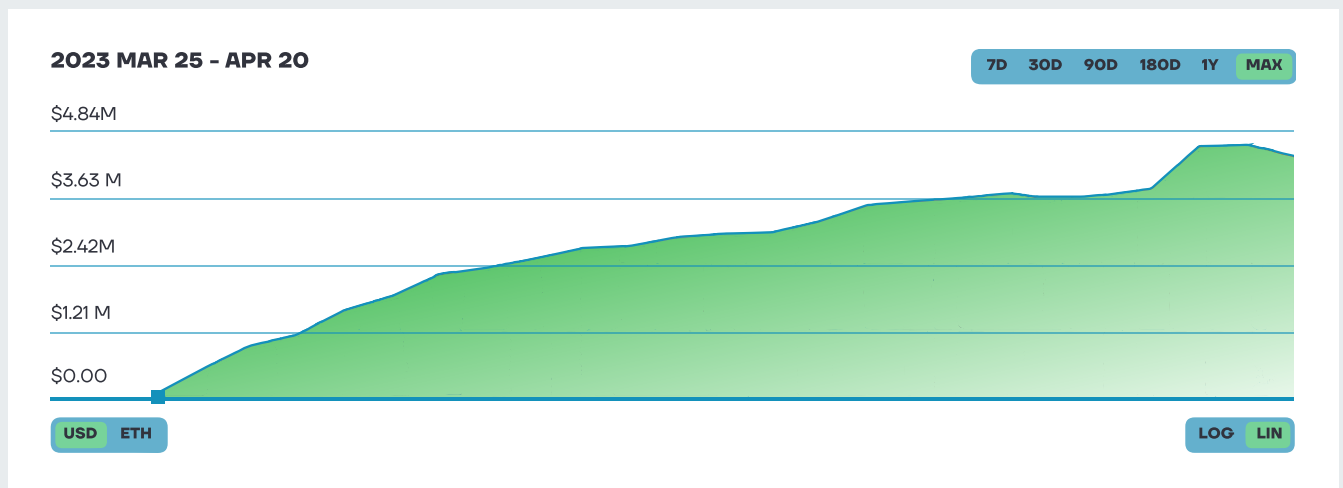


Figure 37: Polygon zkEVM TVL activity

Source: L2BEAT

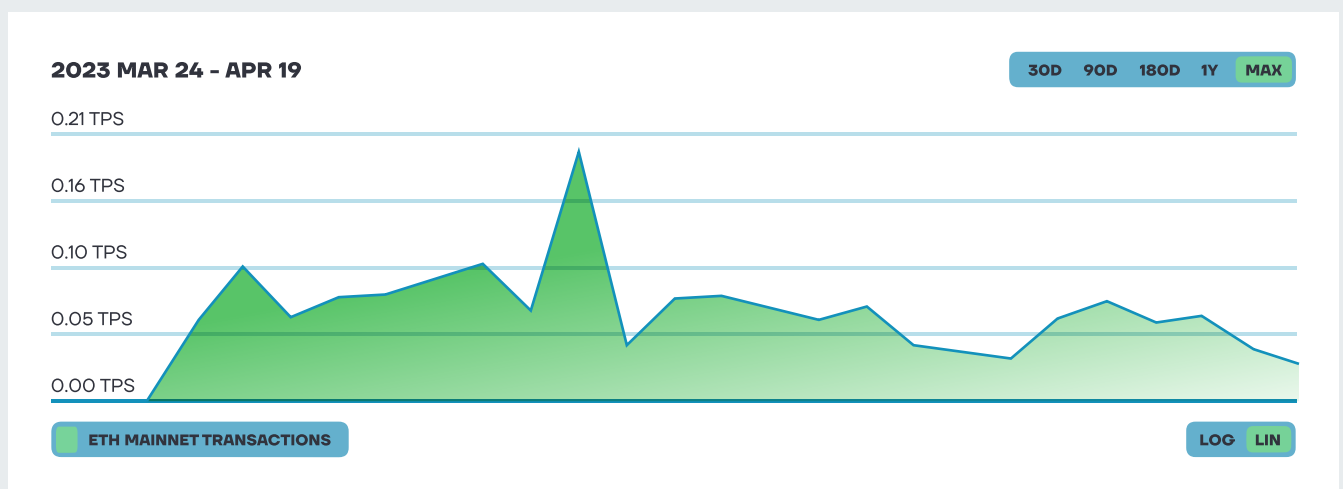


Figure 38: Polygon zkEVM network activity

Source: L2BEAT

## COMPARISON TABLE

### ZK-ROLLUP ECOSYSTEM

NAME	ZKP	DEVELOPMENT STAGE	EVM-COMPATIBILITY	CODEBASE	TOKEN	FUNDRAISING	TVL 27.06.23
zkSync	ZK-SNARK (Plonk)	Mainnet	zkEVM type 4, via SDK and intermediate solutions, claimed compatibility = 99%	Solidity, Vyper, Rust, Yul (via compilers). Zinc (native programming language).	Gas Fees in ETH and another tokens. Native token - for validators and staking. No more data	\$458M total, of which \$200M for ecosystem development	\$725M
StarkNet	ZK-STARK	Testnet	zkEVM type 4, its own VM. A number of Warp-like SDK solutions are under development, allowing to compile Solidity and other languages into native Cairo code.	Solidity, Rust, Python (via compilers). Cairo (native programming language)	Gas Fees in ETH. Native token - for validators and staking. No more data.  In the future, the possibility of paying for gas with other tokens is planned.	\$270M+	\$532M
Scroll	ZK-SNARK (Plonk)	Testnet	zkEVM 2-3rd type	Solidity, Rust, Go.	No data. Gas fees in ETH.	\$80M+	No data
Aztec	ZK-SNARK (Plonk)	Aztec Connect is closed	zkEVM type 4	Noir (native programming language).	No data.	\$117M	\$9.4M
Polygon zkEVM	ZK-STARK+ ZK-SNARK	Mainnet	zkEVM Type 3 (approaching Type 2)	-----	Gas fees in ETH	Funding by the Polvaon Thesis program	\$43M

Figure 39: ZK-Rollups Ecosystem



Interestingly, as the network develops, the workload increases and developer activity increases, the price of gas goes down:

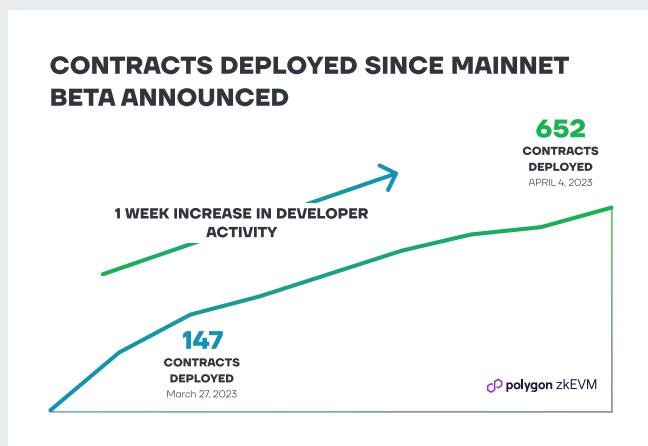


Figure 40: Contracts deployed since mainnet beta announced

Source: Polygon Labs “Tracking the Journey: What’s Really Happening on Polygon zkEVM Mainnet Beta?”

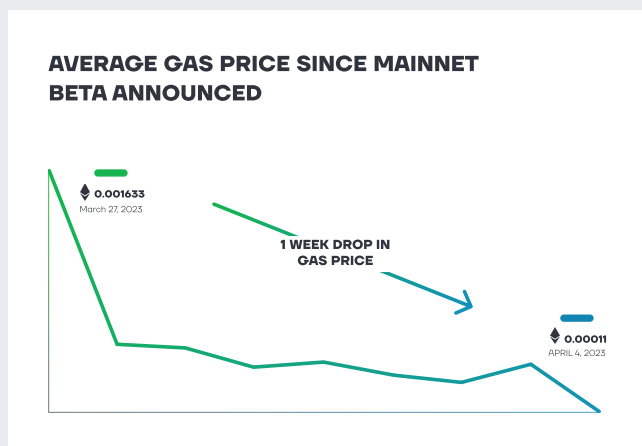


Figure 41: Average gas price since mainnet beta announced

Source: Polygon Labs “Tracking the Journey: What’s Really Happening on Polygon zkEVM Mainnet Beta?”

“



**KOSTAS FERLES**  
CRO at Veridise



Veridise is a blockchain security company founded by a team of world-class researchers. They are passionate about bringing state-of-the-art security research and software analysis tools to the fingertips of web3 developers. Veridise is a proven leader in auditing Zero-Knowledge Circuits, Smart Contracts, and Blockchains.

## Zero-knowledge and Web3. Why now?

Zero-knowledge systems are crucial in today’s digital world where privacy and security are paramount. They allow parties to share information with each other without revealing any sensitive details and are particularly valuable for blockchains. While blockchains provide a transparent and immutable record of transactions, they also pose privacy concerns, as all information stored on the blockchain is visible to all participants.

ZK systems can solve this by allowing for the creation of private blockchains, where some information is kept hidden from certain participants, facilitating keeping sensitive information, for instance, personally identifiable information or trade secrets to not be exposed to unauthorized parties.

Additionally, ZK systems can be used to improve the scalability and efficiency of blockchains. They help reduce the amount of data that needs to be transmitted and stored on the blockchain, while still maintaining the security and integrity of the system.

## Veridise’s contribution to ZK

The history of web3 has shown us that building a secure system is no easy feat. The introduction of ZK systems has added yet another layer of complexity. Developers of ZK-based web3 applications must not only develop two separate components, ZK and eeb3, but also ensure that the interaction between the two is correct, seamless and secure. At Veridise, our team of program analysis and security experts is constantly developing new solutions to keep your favorite ZK and web3 systems secure.

Among clients:



RIBBON



MANTA NETWORK



Scroll



ankr

Backed by:

POLYCHAIN CAPITAL



galaxy

啟明創投  
QIMING VENTURE PARTNERS

CoinDCX Ventures



Hack VC



MONOCEROS



dao5



ANGEL INVESTORS

”



## UNIQUE DEPOSITORS POLYGON ZKEVM DEPOSITS

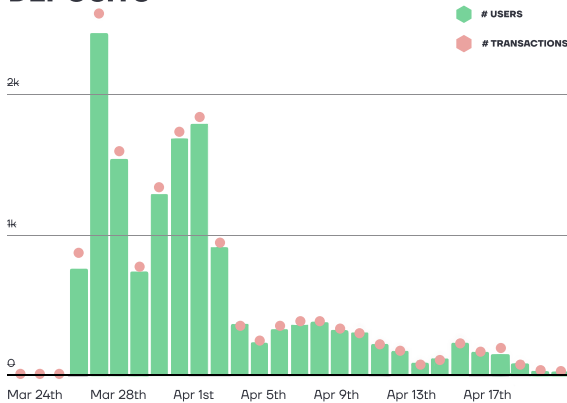


Figure 42: Unique depositors Polygon zkEVM  
Source: Dune analytics

## POLYGON ZKEVM DEPOSITS \$

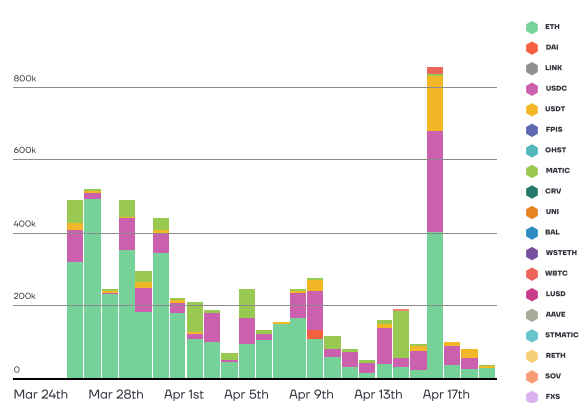


Figure 43: Polygon zkEVM deposits  
Source: Dune analytics

66



### CIRCLE FANG

ZK Researcher at  
Antalpha Ventures

## ANTALPHA VENTURES

Antalpha Ventures invests in the world's future infrastructure for Web 3.0, blockchain and digital asset technology.

Zero Knowledge Proof is a groundbreaking primitive closely aligned with blockchain, as they were both introduced to achieve trustlessness. Even though nowadays, many ZK use cases remain within the crypto society to address scalability and privacy issues, however, its potentials are yet to be unlocked in other areas such as machine learning, data/identity privacy, IoT, and supply chains. ZK is an industry standalone, and it has the potential to surpass the market size of blockchain and crypto.

### Here are the reasons why:

Blockchain and ZK are both powerful tools for obtaining trust. Blockchain maintains a truthful ledger, whereas ZK is used to prove that the computation was processed correctly.

The ZK industry is evolving rapidly. Researchers and teams are constantly working on better crypto primitives to make ZK more efficient and widely adopted. Just four years ago, we only had Groth16, and now we have Plonk, Marlin, Nova, Hyperplonk, and Hypernova. Additionally, many talented teams are pushing for ZK hardware acceleration to enhance the efficiency and accessibility of this crypto primitive.

Artificial intelligence is transforming the world. Inevitably, we will live in a more autonomous world in 10 years, and our lives will become more dependent on algorithms. ZK is a powerful tool that can be utilized to enforce rights and justice against the big machines.

Among portfolio:



SEBA BANK

WOO



Scroll



Orderly Network

TRIBE CAPITAL

99



## CONCLUSION

At the moment, there is a race between L2 solutions on Ethereum, with optimistic rollups having the largest TVL and ecosystem and offering native EVM compatibility. However, they have lower bandwidth and security than ZK solutions. Among ZK solutions, Starkware and zkSync are the two strongest contenders, with established ecosystems and toolkits, but there is also a downside to them: architectural and development complexity. Scroll and Polygon zkEVM, on the other hand, are working on better EVM compatibility.

**By Vitalik Buterin:** Overall, I think in the short term, optimistic convolutions will probably win for general-purpose EVM computing, and ZK convolutions will probably win for simple payments, exchanges, and other application-specific use cases, but in the medium, to long-term, ZK convolutions will succeed in all use cases as ZK-SNARK technology improves.

In the evolving landscape of ZKR, we witness the first steps of promising ZK-STARK technology. However, it's important to acknowledge that ZK-SNARKs continue to advance, closing the gap with ZK-STARKs through the trusted setup and quantum resistance improvements. Nevertheless, challenges persist regarding high costs and Sequencers centralization. But, we are optimistic about Zero-Knowledge, and these issues can be optimized soon.

Furthermore, it's important to highlight several other early ZK protocols, including Spartan, Succinct Aurora, RedShift, AirAssembly, Hyrax, Kopis, Lakonia, and more. Future solutions can incorporate combinations of different ZK-proofs and architecture components, blending low gas costs with high speed and optimal proof size with good EVM compatibility or in-build projects ecosystem.

We are currently witnessing the flourishing era of optimistic rollups, which have already demonstrated the advantages of EVM compatibility and cost-effective transactions. ZK-rollups are the next significant milestone in the development of layer-2 solutions for Ethereum. It is evident that by optimizing these solutions, we can achieve enhanced security and user-friendliness. Many new projects in this domain are learning from past mistakes and designing more advanced rollup architectures. In the near future, we can expect a competitive race among layer-2 ecosystems. There is a possibility of establishing cross-rollup connections, allowing for interconnectivity between different rollup solutions based on the specific functional requirements of users. This dynamic evolution is driving the development of more efficient and interconnected L2 ecosystems.

“The ZK-rollup ecosystem holds great potential in addressing scalability and privacy concerns in blockchain networks. Its implementation allows for secure and efficient transaction processing, while ensuring the protection of user privacy. This approach has already been successfully utilized in several blockchain networks and applications, from DeFi to NFTs, and other use cases where achieving scalability and privacy are critical objectives. Currently, there are many ZK-protocols under active development, and it is likely that combinations of different ZK-proof variants may be used in the future.

With the ZK-rollup ecosystem, we are only at the beginning of the great transformation of crypto. Enabling Ethereum and other blockchains to handle thousands of transactions per second, this technology will allow for faster and more cost-effective transactions. The significance of ZK-rollups for crypto is immense, as it will ensure the scalability, privacy, and security of blockchain networks, making them more useful and efficient for everyday use cases.



**ALEX MUKHIN**

Co-Founder and Managing Partner  
at Cryptomeria Capital



# ABOUT THE AUTHORS

## ABOUT THE AUTHORS



**VADIM KREKOTIN**

Founding Partner



**ALEX MUKHIN**

Managing Partner



**IVAN SEMENOV**

Managing Partner



**GRIGORIY MURRBAN**

Associate



**ALEXEY STELMAKH**

Research Assistant

## ABOUT CRYPTOMERIA CAPITAL

Cryptomeria Capital is an early-stage VC firm based in Dubai with presence in Singapore and Hong-Kong. 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. Joseph Poon, Vitalik Buterin Plasma: Scalable Autonomous Smart Contracts, <https://plasma.io/plasma.pdf> 11.08.2017
2. Ashwin Ramachandran The Life and Death of Plasma, Dragonfly Research 27.01.2020
3. Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell Bulletproofs: Short Proofs for Confidential Transactions and More, eprint.iacr 22.12.2017
4. Lucas Nuzzi Monero Becomes Bulletproof, Digital Asset Research 18.10.2018
5. Cathie Yun Programmable Constraint Systems for Bulletproofs, Interstellar 20.11.2018
6. StarkWare Team Validity Proofs vs. Fraud Proofs, StarkWare Blog 23.01.2019
7. Elements Team Confidential Transactions, [elementsproject.org](https://elementsproject.org)
8. StarkWare Team Fractal Scaling: From L2 to L3, StarkWare Blog 21.12.2021
9. <https://www.zkrollups.xyz/>
10. Maven11 Research The Modular World, Maven11 Substack 14.03.2022
11. Vitalik Buterin An Incomplete Guide to Rollups, [vitalik.ca](https://vitalik.ca) 05.01.2021
12. Vitalik Buterin \*\*\*\*On-chain scaling to potentially ~500 tx/sec through mass tx validation, \*\*\*\*[ethresear.ch](https://ethresear.ch) September 2018
13. StarkWare Team Validity Proofs vs. Fraud Proofs Strike Back, StarkWare Blog 05.12.2019
14. Alchemy Team How Do Optimistic Rollups Work (The Complete Guide), Alchemy Blog
15. William Doom Optimistic Rollups, [ethereum.org](https://ethereum.org) 07.04.2023
16. Arbitrum Dev Center FAQs: Protocol, [developer.offchainlabs](https://developer.offchainlabs.com)
17. New Order An Overview on ZK Rollups and zkEVM, New Order Medium 22.08.2022
18. Matter Labs zkSync 2.0: Hello Ethereum!, Matter Labs Medium 31.05.2021
19. <https://github.com/matter-labs/awesome-zero-knowledge-proofs>
20. Mary Maller Introducing Sonic: A Practical zk-SNARK with a Nearly Trustless Setup, Bentham's Gaze 07.02.2019
21. Metastate Team Demystifying Fractal: Part I [research.metastate.dev](https://research.metastate.dev) 08.04.2020
22. Thomas Walton-Pocock PLONK Benchmarks I — 2.5x faster than Groth16 on MiMC, \*\*\*\*\*Aztec Network 18.12.2019
23. Daniel Benarroch Diving into the zk-SNARKs Setup Phase, QEDIT 07.02.2019
24. Eli-Ben Sasson A Cambrian Explosion of Crypto Proofs, [Nakamoto.com](https://nakamoto.com) 08.01.2020
25. Shihui Fu, Guang Gong Polaris: Transparent Succinct Zero-Knowledge Arguments for R1CS with Efficient Verifier, Sciendo 31.05.2021
26. msfew.eth zk, zkVM, zkEVM and their Future, [mirror.xyz](https://mirror.xyz) 24.05.2022



## BIBLIOGRAPHY

27. Joe Andrews An Introduction to AZTEC, Aztec Network blog 17.05.2019
28. Aztec Network Documentation <https://docs.aztec.network/>
29. Jon Wu Explaining the “Network” in Aztec Network, Aztec Network blog 20.09.2022
30. <https://scroll.mirror.xyz/>
31. David Schwartz \*\*\*\*Proof of Efficiency: A new consensus mechanism for zk-rollups, [ethresear.ch](https://ethresear.ch) 12.02.2022
32. Polygon ZK: Deep Dive Into Polygon Hermez 2.0, Polygon Team
33. Trapdoor-Tech L2 — Deep into zkSync Source Code, 01.11.2020
34. Polygon zkEVM Documentation <https://docs.hermez.io/zkEVM/Overview/Overview/>
35. Polygon Team Polygon Announces Polygon Miden - A STARK-Based, Ethereum-Compatible Rollup, [polygon.technology](https://polygon.technology) 16.11.2021
36. Pedro Polygon Miden Deep Dive: A STARK Based zk-Rollup, [medium.com](https://medium.com) 25.02.2022
37. <https://github.com/OxPolygonMiden/miden-vm>
38. Thomas Lavour, Jérôme Lacan, Caroline P. C. Enabling Blockchain Services for IoE with Zk-Rollups, [mdpi.com](https://mdpi.com) 29.08.2022
39. Ariel Gabizon, Zachary J. Williamson, Oana Ciobotary Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge, eprint.iacr 21.08.2019
40. Alessandro Chiesa, Yuncong Hu, Mary Maller, Pratyush Mishra, Psi Vesely, Nicolas Ward Marlin: Preprocessing ZK-SNARKs with Universal and Updatable SRS, eprint.iacr 27.05.2020
41. Alessandro Chiesa, Dev Ojha, Nicholas Spooner FRACTAL: Post-Quantum and Transparent Recursive Proofs from Holography, eprint.iacr 23.09.2019
42. Alexander Golovnev, Jonathan Lee, Srinath Setty, Justin Thaler, Riad S. Wahby Brakedown: Linear-time and post-quantum SNARKs for R1CS, eprint.iacr 16.08.2021
43. Ahmed Kosba, Dimitrios Papadopoulos, Charalampos Papamanthou, Dawn Song MIRAGE: Succinct Arguments for Randomized Algorithms with Applications to Universal zk-SNARKs, [usenix.org](https://usenix.org) 12.08.2020
44. Dune Analytics <https://dune.com/Marcov/zkSync> (добавить дату)
45. Dune Analytics <https://dune.com/fennec/Stark-Gate>
46. Dune Analytics: <https://dune.com/gm365/L2>
47. L2beat: <https://l2beat.com/>
48. StarkEx Documentation: <https://docs.starkware.co/starkex/overview.html>
49. koala1992 Comparison of Different zk-SNARKs, [zhuanlan.zhihu.com](https://zhuanlan.zhihu.com) 17.05.2020
50. koala1992 Compare zk-SNARKs in practice, [zhuanlan.zhihu.com](https://zhuanlan.zhihu.com) 05.06.2020
51. Ronald Mannak Comparing General Purpose zk-SNARKs, Coinmonks 11.11.2019



## BIBLIOGRAPHY

52. Polygon team Hermes 1.0 Documentation, Polygon zkEVM Documentation
53. O(1) LABS Kimchi: The latest update to Mina's proof system, [minaprotocol.com](https://minaprotocol.com) 10.02.2022
54. Polygon Labs The Polygon Thesis: Strategic Focus on ZK Technology as the Next Major Chapter for Polygon; \$1B Treasury Allocation, [polygon.technology](https://polygon.technology) 13.08.2021
55. Georgia Weston Zero-Knowledge Rollups – Simply Explained, [101blockchain.com](https://101blockchain.com) 24.06.2022
56. Justin Thaler Snark security and performance, a16zcrypto 13.09.2022

## 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](https://cryptomeriacapital.com)

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