Layer 2 Explained: ZK-Rollups

You might have heard about layer 2 solutions like ZK-rollups that aim to increase transaction throughput on the Ethereum blockchain. But what exactly are ZK-rollups, and how do they work? **ZK-rollups are a type of layer 2 solution that moves computation off-chain, reducing congestion and increasing throughput of the Ethereum blockchain.** In this article, we'll explore ZK-rollups and their advantages over Optimistic rollups, how ZK-rollups enhance privacy, and enable cheaper gas fees and higher efficiency for Ethereum. We'll also take a look at some of the popular ZK-rollup blockchain projects, such as zkSync, StarkNet, and Polygon Zero.

What are ZK-Rollups?

Zero-knowledge rollups (ZK-rollups) are layer 2 solutions that increase throughput on the Ethereum blockchain by moving computation and state off-chain. ZK-rollups, and its close competitor optimistic rollups, are two leading solutions to solve the congestion issue on the Ethereum blockchain.

A zero-knowledge proof is a method of establishing the truth of a proposition without exposing it. ZK rollups are like an express lane at a toll booth. Imagine if every car had to stop at the toll booth and the drive has to show the driver license and pay individually, the process would be time-consuming, and the queue would be long.

ZK rollups are like an express lane at a toll booth. Photo source: Hong Kong Autotoll

Now, on the express lane, the system instantly detects the car plate for record-keeping purposes, eliminating the need for individual payments on site. The system efficiently bundles all the pending payments within a given period (say, in an hour) into batches. And then, it settles each payment batch with the bank by deducting the corresponding amount from the car owners' accounts. This process greatly reduces the transaction turnaround time on the lane, leading to a swift and seamless flow of traffic.

How ZK-rollups work

Basically, ZK-rollups bundle transactions into batches. The operators then submit a summary of the changes to represent all the transactions in a batch. The summary data defines the changes that should be made to the Ethereum blockchain and some cryptographic proof that those changes are correct.

ZK-rollups employ validity proofs to compute transactions off-chain and compress hundreds of transactions before posting cryptographic validity proofs on the Ethereum blockchain.

Additionally, ZK-rollups compress data to reduce the amount of data posted to Ethereum and inherit the security of the base-layer network for settlement.

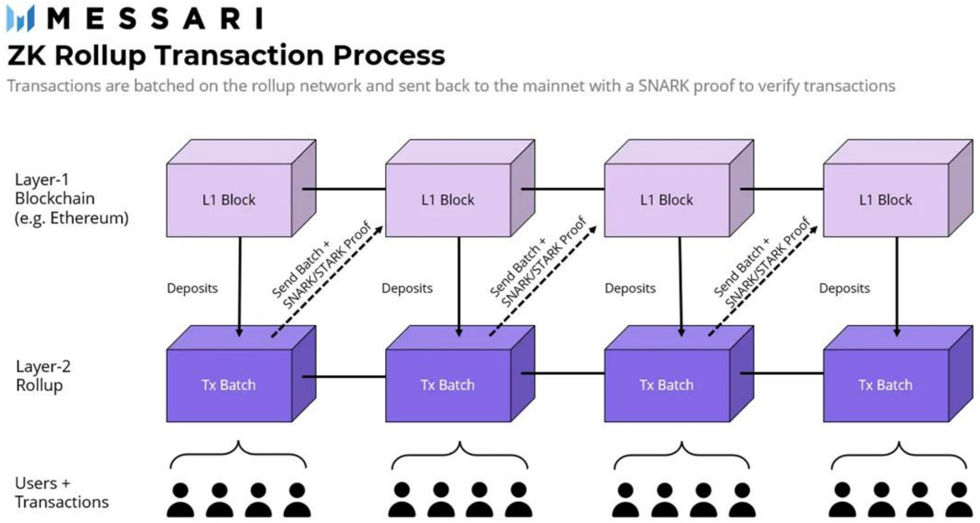
MESSARI
ZK Rollup Transaction Process
Transactions are batched on the rollup network and sent back to the mainnet with a SNARK proof to verify transactions
Layer-1 Blockchain (e.g. Ethereum)
L1 Block
L1 Block
L1 Block
L1 Block
Deposits
Send Batch + SNARK/STARK Proof
Deposits
Send Batch + SNARK/STARK Proof
Deposits
Send Batch + SNARK/STARK Proof
Deposits
Layer-2 Rollup
Tx Batch
Tx Batch
Tx Batch
Tx Batch
Users + Transactions

Photo illustration of the ZK-rollup transaction process. Source: Messari.

Sum up in a sentence: A ZK-rollup executes transactions and processes data, while Ethereum receives and stores only the bare minimum results on-chain.

These advantages make ZK-rollups promising to support all existing decentralised applications (dapps) and services smoothly.

ZK Rollups vs Optimistic Rollups

When it comes to scaling solutions for layer 2 of Ethereum, two main approaches have emerged: ZK-rollups and Optimistic rollups. While both approaches aim to increase the transaction throughput of the underlying blockchain, they differ in their mechanisms. As a popular comparison, what are the difference between Optimistic rollups and ZK-rollups?

Optimistic rollups utilize fraud proofs that allow any user to challenge the outcome of a rollup execution during a specific time window. In contrast, ZK-rollups use validity proofs. This means that validating a block is much faster on ZK-rollups, as they only need the validity proof instead of all transaction data, as is the case with Optimistic rollups.

Therefore, withdrawal periods are significantly shorter for ZK-rollups, and on-chain gas costs per transaction are lower, comparing with Optimistic rollups. However, off-chain computation costs for ZK-rollups are higher, and they are more complex to implement due to the new and mathematically sophisticated technology of ZK-SNARKs.

While Optimistic rollups have had a head start in terms of adoption due to their relative simplicity, proponents of ZK-rollups consider them a more optimal long-term solution for scalability, thanks to their usage of cryptographically verifiable validity proofs.

In 2021, a blog post written by Ethereum co-founder, Vitalik Buterin, expressed his opinion on the future of ZK-rollups. He stated that he believes that ZK-rollups will win out –against its close competitor optimistic rollups – in all use cases in the medium to long term as ZK-SNARK technology improves.

Ethereum co-founder Vitalik Buterin spoke at Ethereum Development Conference EDCON 2023 in Montenegro, highlighting the significance of ZK-SNARK in the future development of blockchain. Source: BlockTempo.

How ZK Rollups enhances Privacy for Ethereum

Most blockchains are public, this makes privacy a critical concern in the blockchain world. ZK-rollups have an advantage in this area, as they can prove that a transaction is valid without revealing information such as wallet addresses and values on the Ethereum mainnet.

One key feature of ZK-rollups is the ability to leave off-chain any transaction data that is only used for verification and not relevant to computing the state update. This reduces the amount of information published on-chain, enhancing privacy.

ZK-rollups use validity proofs, which include a cryptographic proof called a ZK-SNARK, proving the result is correct. ZK-SNARKs are a new and mathematically complex technology that allows one party to prove they know a value without disclosing any other information about it. This protects the privacy of the party providing the proof, as the verifier cannot derive any additional information from the proof beyond the fact that the value is known.

The acronym zk-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," and it refers to a proof construction in which one can prove possession of certain information.

ZK-SNARKs ensure transaction security and privacy. Here is a breakdown of each term in the zk-SNARK acronym.

ZK: Zero Knowledge.	No additional information is required other than the transaction's validity.
S: Succinct, which means short.	The proof size is small, resulting in transactions being processed quickly and easily.

	This feature allows Ethereum to process more transactions.
N: Non-interactive.	No interaction with the people who verify the work or transactions is required.
ARK: Argument of Knowledge.	The checker's validity proof (that these transactions are legitimate) is correct. This section denotes the computational strength of ZK-SNARKS.

How does ZK-SNARK work?

- To use ZK-SNARK, the prover generates a pair of keys (public and private), and signs the transaction using the private key. The transaction is then encoded into a zk-SNARK, which serves as a mathematical proof that it is valid.
- This proof is sent to the verifier along with the public key.
- The verifier checks the formula using the public key, without learning any other information about the transaction.

To illustrate the concept of ZK-SNARK, let's imagine a scenario where you are purchasing alcohol from a store. At the checkout, you need to present an ID to verify that you are of legal drinking age. However, you may not want to reveal all your personal information, such as your ID number and photo, to the staff and anyone nearby.

In this case, to protect your privacy, you use a sticker (or your finger) to selectively obscure all other information on the ID except for the necessary data, such as your birth year. With this approach, the cashier can verify your age and you don’t reveal any extra information. This is similar to how ZK-SNARK works, where it provides a way to prove that you have certain information, such as a valid transaction, without revealing any other sensitive information.

Using your finger to obscure your ID number on the ID card. Source: Hong Kong government.

With ZK-SNARKs technology, ZK-rollups can also support confidential transactions for token transfers at the protocol level by default. Privacy-focused cryptocurrencies like Zcash have already adopted ZK-SNARKs.

ZK-SNARKs technology provides a way to validate credentials or identities without revealing sensitive information. Other promising applications of ZK-SNARKs include identity verification, voting systems and many more.

How ZK Rollups Enables Cheaper Gas Fee for Ethereum

ZK-rollups are a new technology that increases the scalability of the blockchain while keeping transaction costs low and maintaining the security of the layer 1 network (Ethereum). ZK-rollups achieve this by taking computation off-chain and compressing transaction data. They use compression techniques to reduce transaction data, such as representing accounts with an index instead of an address.

By compressing transaction data, ZK-rollups significantly increase the number of transactions processed per block, thus increasing throughput. They reduce transaction costs by batching transactions and spreading fixed costs across multiple users.

However, ZK-rollups have higher off-chain computation costs, especially for ZK-SNARK proving, which can be expensive. ZK-rollup operators must produce validity proofs for transaction batches, which is resource-intensive. Verifying zero-knowledge proofs on the Ethereum mainnet also costs “gas”.

Gas is the amount of computational effort required to execute specific operations on blockchain networks like Ethereum.

Having said that, ZK-rollups decrease user transaction costs due to the fixed cost of proof verification, which is a significant benefit not offered by traditional blockchain environments.

Gas fee status about layer 2 blockchain solutions on the Ethereum blockchain according to L2Fees. Source: L2Fees, as of May 31st, 2023.

Exploring ZK-rollup Projects

What are the popular ZK-rollup blockchain projects? Top Ethereum ZK-rollup projects including zkSync, StarkNet, Polygon Zero and Loopring have made significant strides in lowering costs and enabling frictionless user experience on wallets, dapps and more.

ZK-rollup Blockchains	**Brief Information***	**Official Website**
zkSync Era	Layer 2 protocol that scales Ethereum with	https://zksync.io/

	cutting-edge ZK tech	
StarkNet	Decentralised layer 2 network that enables Ethereum to scale securely	https://www.starknet.io/en
Polygon Zero	ZK-rollup solution that aims to reduce the computational cost of generating validity proofs	https://polygon.technology/polygon-zkevm
Mina Protocol	A project leveraging recursive zero knowledge proofs to enable the world’s lightest, most	https://minaprotocol.com/

	accessible blockchain	
Aztec	Hybrid ZK-rollup supporting both public and private smart contract execution	https://aztec.network/
Loopring	ZK-rollup exchange and payment protocol on Ethereum	https://loopring.org/#/
ImmutableX	Application-specific StarkEx ZK-rollup which facilitates the minting, trading and transferring of NFTs and ERC-20s	https://www.immutable.com/

*Source: Official project websites and social media accounts.

Summary: Future of ZK-rollups

In conclusion, ZK-rollups are a type of layer 2 solution to increase transaction throughput on the Ethereum blockchain by moving computation off-chain. They bundle transactions into batches, compress data and use validity proofs to compute transactions off-chain, resulting in reduced congestion, cheaper gas fees, and higher efficiency. Compared to its close competitor Optimistic rollups, ZK-rollups use faster validity proofs, offer shorter withdrawal periods, and provide better privacy protection.

With the adoption of ZK-SNARKs technology, ZK-rollups enable confidential transactions and have promising applications in identity verification and voting systems. Overall, ZK-rollups are a promising solution for supporting all existing decentralised applications and services smoothly.

Sign up for HashKey PRO (Professional Investor only)

Want to stay on top of the blockchain and digital asset market?

Sign up below to receive HashKey insights and knowledge in your inbox.