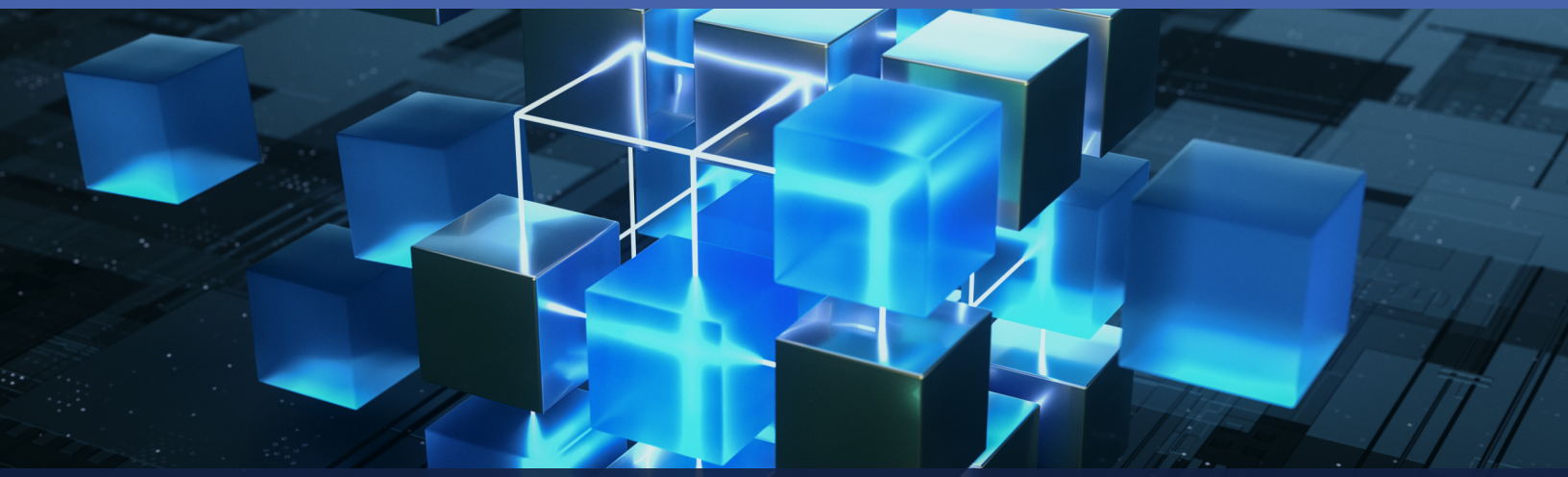

Introduction to Rollups

What are Rollups?

A rollup is a blockchain that processes large bundles of transactions in an optimized environment then transfers the blocks to the Ethereum Mainnet. Rollups can combine hundreds of off-chain transactions into one transaction on the main Ethereum chain. This makes them an effective scaling tool that allows work to be completed away from the congested mainchain at a faster pace and cheaper price.

Background

Ethereum usage has increased immensely in recent years, with more and more business users realizing the value the platform has to offer. With this user growth, however, a key pain point has emerged: network congestion. Many have found that Ethereum network traffic and transaction delays have slowed down projects and increased gas fees, which can create a negative user experience. Rollups offer one solution to this challenge.

Rollups are one example of a class of blockchains known as Layer 2 solutions, which aid with scalability and are built on top of the Ethereum Mainnet, or the primary Ethereum network, also known as Layer 1. Rollups allow many transactions to be consolidated into one transaction on Layer 1. In this way, they have become an effective scaling solution, delivering 10x-100x more throughput than the Mainnet and allowing projects to be executed faster with lower gas costs, two key benefits for businesses. Another key aspect of rollups is that they inherit the security and decentralization properties of the Ethereum Mainnet. This is a big advantage for businesses who don't want the complication of managing those issues separately.

Rollups have two main categories: optimistic rollups and zero-knowledge rollups (ZK-rollups). Both offer increased transaction speeds and lower costs, but their execution mechanisms differ in a key way.

With optimistic rollups, it is *optimistically* assumed that the transactions posted on the rollup are valid. After they post, transactions get checked by individuals working on the Layer 1 Mainnet who are economically incentivized to replay the transactions and confirm they're correct. If transactions are recognized to be invalid – for example, if they claim extra Ether or double spend – the individual can submit a fraud proof to the rollup to challenge the transaction. The bond posted by the rollup operator gets slashed, and the third-party checker receives a reward. In this way, attempts at malicious transactions are quickly spotted and optimistic rollups are kept secure.

The time it takes to carry out these third party checks is called the "dispute time delay" and lasts approximately one week, which is sufficient time for the challengers to detect and report fraud as well as enough time to make any attempted attack exceedingly expensive. The longer the time delay, the more expensive it becomes to attack the network at the infrastructure level, as the attacker must "rent" the power needed to try to prevent the fraud proof from being included in the block.

QUICK TAKEAWAYS

- Rollups are a type of Layer 2 blockchain that enable a large number of transactions to execute in an optimized environment away from the main Ethereum chain.
- Rollups are an extremely effective scalability tool, offering 10x–100x more throughput than the Ethereum Mainnet. Additionally, rollups inherit the security and decentralization properties of the Ethereum Mainnet, a big selling point for businesses.
- There are two main types of rollups: optimistic rollups and zero-knowledge rollups (ZK-rollups). Both offer improved scalability and throughput, as well as lower costs, but they differ in how they validate transactions.

ENTERPRISE ETHEREUM ALLIANCE®

This rent is paid by the hour for the duration of the time dispute delay, making longer windows much more costly for attackers. Another feature of note for optimistic rollups is their high Ethereum Virtual Machine (EVM) compatibility, which allows them to easily create Ethereum-like execution environments and seamlessly port from the Mainnet or any EVM chain to the rollup. Higher EVM compatibility produces a development experience that is closer to that provided by Ethereum.

The main difference with ZK-rollups is that they use cryptography to verify transaction validity, creating what's called a zero-knowledge proof that is posted along with the transaction. Zero-knowledge proofs confirm a transaction's legitimacy using only basic information, thus preserving the privacy of the transaction. Additionally, by utilizing cryptography, ZK-rollups remove the third-party dependency and trust required by optimistic rollups. ZK-rollups can also utilize validity proofs, another tool which delivers improved scalability by allowing for a batch of statements to be verified with a single transaction.

So how do you choose between optimistic and ZK-rollups? Both have pros and cons. Optimistic rollups are a more established technology, have a simpler design, are more battle tested and have high EVM compatibility. Conversely, ZK-rollups are a newer, more complex technology for which implementing the EVM is currently more challenging (although that is changing, with more EVM compatible ZK-rollups becoming increasingly available). However, due to their privacy-preserving, trustless transaction validation, ZK-rollups are widely considered to be more secure, a huge plus for businesses. They are also often speedier. With optimistic rollups, the dispute time delay means it can take a week or more to finalize fund withdrawals. ZK-rollups, on the other hand, enable near-instant fund withdrawal, providing the speed that many businesses consider more favorable.

Whether you choose optimistic or ZK, a rollup's primary business benefit is always scalability. Both types of rollups can combine hundreds of off-chain transactions into one transaction on the Ethereum Mainnet, allowing huge numbers of transactions to execute quickly and avoiding the congestion and high fees common on the Mainnet. The inherited security from Ethereum is also critical, removing any question about security properties and consensus mechanisms for block proposals and freeing builders up to focus solely on execution.

However, despite their advantages, it's important to remember that rollups are still a nascent technology and do carry some risks. Like the Ethereum Mainnet, rollups depend on smart contracts to execute transactions, so as in any smart contract situation, they face the risk of a bug causing execution problems or increasing the chain's vulnerability. Additionally, as it currently stands, the keys to upgrade smart contracts are controlled by the rollup team, which means the contracts could be updated to block withdrawal of funds. Due to this, rollups are not currently censorship resistant. However, as rollup technology continues to develop there is an end goal of ensuring no centralized entity has the power to block fund withdrawals. We're likely to see improvements in this area in the coming years.

While rollups are still relatively new and do pose some risks, their business benefits are hard to deny. Additionally, the Ethereum Foundation has already demonstrated clear confidence in the technology, making rollups a central pillar in Ethereum's roadmap, with many improvement proposals based around their enablement. With this buy-in and the numerous advantages they offer, it's clear that rollups aren't going anywhere and have much to offer businesses of all types.

HOW DO I FIND OUT MORE?

Read: An Incomplete Guide to Rollups, by Ethereum co-founder Vitalik Buterin, as well as the follow-up, The Complete Guide to Rollups, by Delphi Digital.

Watch: The EEA's webinar, Introduction to Layer 2 Scaling Solutions for Ethereum, presented by Tas Dienes of the Ethereum Foundation.

Peruse: The Ethereum Foundation's pages on Optimistic Rollups and ZK Rollups.

View file on web page

About the EEA

The Enterprise Ethereum Alliance (EEA) enables organizations to adopt and use Ethereum technology in their daily business operations. The EEA empowers the Ethereum ecosystem to develop new business opportunities, drive industry adoption, and learn and collaborate.

To learn more about joining the EEA, reach out to james.harsh@entethalliance.org or visit https://entethalliance.org/become-a-member/.

Follow the EEA on Facebook, Twitter, LinkedIn, and YouTube.

ENTERPRISE ETHEREUM ALLIANCE®