

TL; DR

Compared to Optimistic Rollups, ZK-Rollups offer the following advantages:

- Compressed transaction data results in lower L1 gas costs.
- Enhanced security with no need for validators to challenge.
- Faster transaction confirmation speed and shorter withdrawal time.

In addition to these benefits, ZK-RaaS has advantages through network effects:

- ZK-RaaS utilizes [ZK-PoW](#) to provide scalable computational power for numerous ZK-Rollups with decentralized prover network, thereby reducing the cost of ZKP calculations.
- Thanks to the faster transaction finality of ZK-Rollups (in the order of minutes) [native Cross-Rollup Communication \(NCRC\)](#) is possible among ZK-Rollups. This resolves the issue of fragmented liquidity.

What is RaaS?

[Rollups-as-a-Service \(RaaS\)](#) provides an abstraction layer on top of the Rollup framework and SDK, making it easy to deploy, maintain, and build on customized, production-grade specific application Rollups (AppRollups). Similar to SaaS (Software-as-a-Service) products, RaaS allows developers to focus on building the application layer, transforming what used to be a process requiring multiple engineers and dozens of hours into a 10-minute no-code deployment.

There are two main types of Rollups: [Optimistic rollups](#) and [ZK-Rollups](#). They differ in transaction verification and dispute resolution, with distinct advantages and disadvantages. Based on the type of Rollup offered, this article divides RaaS into Op-RaaS

and ZK-RaaS

1. Cost

ZK-Rollups have lower L1 Gas costs compared to Optimistic Rollups.

One of the primary objectives of Rollup solutions is to increase the transaction throughput on L1 and reduce users' gas fees. Both Optimistic rollups and ZK-Rollups achieve this goal by batching transactions and periodically submitting them to the L1. Consequently, they both incur gas fees for submitting data to L1.

- Due to the use of fraud proofs, optimistic rollups need to publish all transaction data on-chain. As a result, they require more gas to submit data batches to the main chain.
- ZK-Rollups, on the other hand, utilize efficient data compression techniques (e.g., using indexes to represent user accounts rather than addresses, saving 28 bytes of data). This helps to lower the cost of publishing transaction data on the underlying chain.

Therefore, ZK-Rollups can save more L1 Gas compared to optimistic rollups.

ZK-RaaS reduces ZKP computation costs with decentralized prover network

However, ZK-Rollups entail additional computation costs for generating zero-knowledge proofs, which is exactly what ZK-RaaS aims to address.

As ZK-Rollups are being adopted on a large scale, generating ZKPs requires significant computational power from hardware and mining machines, including CPUs, GPUs, and FPGAs. [Opside](#) has also introduced the concept of [ZK-PoW](#), involving miners in maintaining zkEVM nodes and performing ZKP calculations. The Opside ZK-PoW protocol is deployed across multiple chains, including but not limited to Ethereum, BNB Chain, Polygon PoS, and Opside Chain itself.

To encourage more miners to participate in ZKP computation tasks, Opside has introduced decentralized prover network and [ZKP's Two-Step Submission Algorithm](#). The PoW reward share corresponding to a ZKP is distributed to the submitter of valid ZKPs, which are the miners, following specific rules.

[

1280×462 75.8 KB

](https://ethresear.ch/uploads/default/original/2X/c/c9bbf2f842bb8980f72b0b0953cca409a6d834d3.png)

1. Submitting Proof Hash: Within a time window, multiple miners are allowed to participate in the calculation of zero-knowledge proofs for a specific sequence. After calculating the proof, miners do not directly submit the original proof. Instead, they calculate the proofhash of (proof / address) and submit this proofhash to the contract.
2. Submitting ZKP: After the time window, miners submit the original proof and validate it against the previously submitted proofhash. Miners whose validation is successful receive PoW rewards, with the reward amount distributed proportionally based on the miner's staked amount.

In Opside, the Two-Step Submission Algorithm for ZKP achieves parallel computation and sequential submission of ZKPs, enabling mining machines to execute multiple ZKP generation tasks simultaneously. This significantly accelerates the efficiency of ZKP generation.

2. Transaction Finality and Fund Efficiency

- Optimistic Rollups: There is a challenge period of up to 7 days in Optimistic Rollups. Transactions are only finalized on the main chain after the challenge period ends. Therefore, Optimistic Rollups have a high latency in terms of transaction finality.
- ZK-Rollups: ZK-Rollups excel in low latency for transaction finality, usually taking just a few minutes or even seconds. Once the operator of the nodes verifies the validity proof, it results in a state update.

Due to the challenge period in optimistic rollups, users cannot withdraw funds before its expiration, causing inconvenience. In contrast, ZK-Rollups lack a challenge period, offering users superior fund/liquidity efficiency, allowing them to withdraw funds at any time.

3. Shared Liquidity

It's worth noting that due to the swift confirmation of transactions in ZK-Rollups, it's possible to achieve trustless communication between ZK-Rollups, allowing all Rollups to share asset liquidity

. However, due to the presence of a 7-day challenge period and fraud proofs, achieving trustless native communication between optimistic rollups is impractical.

Opside's ZK-RaaS platform introduces the [NCRC \(Native Cross Rollup Communication\)](#) protocol, providing a trustless Rollup interoperability solution. The NCRC protocol doesn't involve adding an additional third-party bridge to each Rollup; instead, it transforms the native bridge of ZK-Rollups at the system level. This enables direct utilization of the native bridges of various ZK-Rollups for cross-Rollup communication. This approach is not only more concise and comprehensive but also inherits the absolute security of native bridges while avoiding the complexity and trust costs associated with third-party bridges.

[

1280x577 72 KB

](<https://ethresear.ch/uploads/default/original/2X/7/7ebcb66aefa64d868c30db07ba1cbe272a633500.png>)

Opside has successfully implemented NCRC on the testnet. Anyone can now experience it at <https://pre-alpha-assetshub.opside.network/>.

4. Security

Optimistic Rollups:

Fraud proofs in optimistic rollups protect the blockchain network by relying on honest validators to ensure the validity of transactions. If there are no honest nodes to challenge invalid transactions, malicious actors could exploit this vulnerability and steal funds, rendering these optimistic rollups insecure.

ZK-Rollups:

ZK-Rollups don't rely on honest validators; instead, they use zero-knowledge proofs to verify transactions. The advantage is that ZKPs provide security assurances through mathematical proofs rather than human participants, making ZK-Rollups trustless.

While fraud proofs in optimistic rollups are theoretically viable and a handful of rollups are currently operational, the risks of this security model are exposed over time as the number of optimistic rollups increases. This risk could become a "grey rhino" or even a "black swan". Running an honest validator incurs costs and is mostly unprofitable. When Op-RaaS creates numerous optimistic rollups, beyond a few leading rollups, ensuring honest nodes for each rollup becomes challenging, particularly for those with less attention

On the other hand, the security of ZK-Rollups is trustless, as they don't rely on users or validators to challenge fraudulent transactions. Instead, they provide security guarantees through mathematical proofs.

Conclusion

Whether it's ZK-RaaS or Op-RaaS, developers can have their own Rollup application chains without the need to manage complex software and hardware.

ZK-RaaS platforms like [Opside](#), representing ZK-RaaS, have introduced features such as ZK-PoW and the NCRC protocol, which further highlight the advantages of ZK-Rollups.

[

image

1542×1206 188 KB

](https://ethresear.ch/uploads/default/original/2X/4/4f418b0bca6c38901983cd734ff4e43624017ffc.png)