Optimistic Rollups Vs. Zero-Knowledge Rollups

No comments

Over the past few years, Ethereum has created good prospects for many sectors and significant setbacks. Ethereum has enabled many innovative trends, such as DeFi and NFTs, to flourish. Ethereum and the decentralized ecosystem are gradually expanding with new applications and innovation. However, the radical increase in network activity has also led to a debate over-optimistic rollups and ZK rollups over which scaling solution is best. Ethereum transactions are becoming increasingly expensive every day, which urgently necessitates scaling. Although rollups have important security properties and significant trust assumptions, they can offer great scalability. The difference between the two layer 2 scaling solutions can assist you in choosing the best option. The following post discusses the differences between optimistic and ZK rollups in detail.

What is a Rollup?

In rollups, transactions are processed off-chain, primarily on a rollup-specific chain, then batch-compressed and delivered to the main Ethereum chain. This eases the strain on the main Ethereum network. Rollups are Ethereum's scaling solution that takes transactions off the main blockchain, where they are processed, and sends SNARKs back to it. These SNARKs then verify transactions on the main blockchain.

Types of Rollups

Using rollups as one of the most promising Layer 2 solutions is becoming increasingly popular. However, since rollups offload transaction calculations to a third-party server and store transaction data on the Ethereum blockchain, they are protected by Layer 1. In the context of rollups, there are two main types: Zero-Knowledge (ZK) and Optimistic. The main difference between these two types of rollups is the verification process. Validity proofs are generated for each batch of transactions in ZK rollups and sent to the main chain for validation. Cryptographic proofs are generated to verify the legitimacy of transactions in ZK rollups.

What is Zero Knowledge Rollups?

With Zero Knowledge Rollups (ZK Rollups), Ethereum smart contracts execute numerous transactions off of the main blockchain to expand the network. A ZK Rollup aggregates or rolls up hundreds of off-chain transfers into a single transaction. as proof of validity, it returns a SNARK (short non-interactive argument of knowledge) to the main chain. This way, ZK Rollups are faster and cheaper to confirm transactions than hefty transaction data since only the validity proof is stored on the Ethereum network. A zero-knowledge technique involves verifying something without disclosing or sharing the underlying facts. A payment app could be used to determine if there are enough funds in your bank account to make a transaction without knowing anything about it. Or a program could verify a password's authenticity without processing it. Zero-knowledge proofs can help broker important agreements, transactions, and interactions more privately and securely.

What is an Optimistic Rollup?

Optimistic rollups are a method of scaling Ethereum that involves moving computation off-chain and storing state off-chain. Transactions run outside of Ethereum, but the call data is posted to the Mainnet. Before submitting multiple off-chain transactions to Ethereum, optimistic rollup operators bundle them together in large batches. This way, fixed costs are spread across various batch transactions, reducing end users' fees. Optimistic rollups reduce Ethereum's data upload limit by using compression techniques. Off-chain transactions are assumed to be valid in optimistic rollups, but on-chain transaction batches do not receive cryptographic proof of validity. As a result, optimistic rollups differ from zero-knowledge rollups, which publish cryptographic proofs of validity. Instead of detecting cases of incorrect calculation of transactions, optimistic rollups employ a fraud-proofing scheme. Ethereum offers a time window (called a challenging period) during which anyone can challenge the results of a rollup transaction by devising fraud-proof.

When the fraud-proof is successful, the rollup protocol re-executes the transaction(s) and updates the rollup's state accordingly. As a result of a successful fraud-proof, a penalty will be added to the block of the sequencer that included the incorrectly executed transaction. The rollup batch is considered valid and accepted on Ethereum if it remains unchallenged (i.e., all transactions are correctly executed) after the challenge period has expired. There are caveats to building on an unconfirmed rollup block: transaction results will be reversed if they are based on an incorrectly executed transaction previously published.

Zero-Knowledge vs. Optimistic Rollup Comparison: Key Differences

It gives the impression that optimistic rollups are faster and more cost-effective than zk rollups from a generic perspective. However, their differences must be compared based on a variety of critical factors, such as transaction finality, DeFi readiness, security, transaction costs, and user experience. The following is a comparison of layer 2 scaling solutions.

image not found or type unknown optimistic Vs. ZK Rollups Optimistic Rollups Vs. Zero-Knowledge Rollups

1- Ready for DeFi

Most DeFi applications use the Ethereum blockchain. Optimistic rollups such as Optimism and Arbitrum use execution models similar to Ethereum Virtual Machines. No matter how complex the code is, developers can switch to optimistic rollups easily. Due to the recently-improved documentation of Arbitrum, you are less likely to encounter problems when migrating applications. Therefore, you are more likely to achieve the functionality of alternative EVM-supported scaling solutions in optimistic rollups. However, ZK rollup protocols face a significant compatibility issue. The requirement for validity proofs for each type of transaction in ZK rollups complicates the development of rollup technologies. Zero-knowledge rollups have shown promising results in discrete tasks such as trading and direct transfers. DeFi smart contract general-purpose support still needs to be developed. However, the optimism vs. ZK rollup comparison cannot turn completely in favor of optimistic rollups for DeFi readiness. as a recent update provided support for EVM compatibility, ZK rollups could also catch up to optimistic rollups in terms of functionalities.

2- Transaction Finality

Comparison of optimistic and zero-knowledge layer 2 rollups would also reflect on transaction finality. How fast can tokens be withdrawn in layer 2 transactions? There could be a major disadvantage to optimistic rollups in this case since the challenge period is delayed by one week. Users must complete a challenging period before withdrawing their funds, resulting in a delay in transaction completion. In contrast, zero-knowledge rollups allow for immediate withdrawal of funds due to validity proofs. The validity proofs provide unquestionable proof of off-chain transactions, so users do not have to wait long before withdrawing funds.

3- Programming Simplicity

Programming ease is also an important factor when comparing ZK rollups vs. optimistic rollups. For easier programming, you can look for optimistic rollups with data compression flexibility and EVM compatibility. Ethereum's main network data is published as 'calldata' thanks to the data compression advantages of compressing transaction data with optimistic rollups. While you have to incur slightly higher rollup costs, you can easily compress and program data. On the other hand, ZK rollups do not require publishing transaction data on Ethereum. The ZK-STARKs and ZK-SNARKs are responsible for verifying the accuracy of the rollup state. However, programming ZK rollups that require clear cryptographic proof is challenging.

4- Costs of Transactions

The costs of optimistic rollups are significantly optimistic, as they only invest in the areas that are relevant to scalability. In addition, rollup costs are considerably lower since optimistic rollups require minimal data to be published on Ethereum. Since optimistic rollups do not require proof for transactions unless challenged in special cases, they are likely to be more cost-efficient. As well as supporting EIP-4844 protocols, users can also save money on optimistic rollups. On the other hand, a zero-knowledge rollup is more expensive because of the computational proof required. As a result of the costs associated with creating and verifying proof for each block of transactions, overhead is generated. Additionally, it is essential to note that creating zero-knowledge proofs requires high-end hardware. With the high costs associated with on-chain verification, zk rollups are evidently more expensive than optimistic ones.

5- Trust

As a result of a combination of different factors, trust is also an essential determinant in the Ethereum layer 2 comparisons. For optimistic rollups, a trusted setup is not required. However, ZK rollups need a trusted setup to achieve the desired functionality.

6- Security

Security is the most crucial difference in comparing optimistic and ZK rollups. It is dependent on crypto-economic incentives for users to ensure rollup security that optimistic rollups are secure. Verifiers, for example, would receive rewards for successful fraud-proof submissions. By contrast, zero-knowledge rollups rely on cryptographic proofs of security. Therefore, both types of rollups compete for security.

Final thoughts

By comparing optimistic rollups with zero-knowledge rollups, it is clear that both solutions serve distinct purposes. Due to the use of cryptographic proofs, zero-knowledge rollups appear to be more secure than optimistic rollups. Nevertheless, with the introduction of new crypto-economic incentives for users, security concerns for optimistic rollups can be addressed. Meanwhile, optimistic rollups with EVM compatibility are a better fit for DeFi projects. And zero-knowledge rollups can change the narrative around layer 2 scaling.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.

Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP NEWSLETTER RSS FEED