crypto.com

An Overview of Layer Two Solutions

April 2021

crypto.com

Research and Insights

Macro Report

Head of Research and Insights

Kendrick Lau

RESEARCH DISCLAIMER

This report alone must not be taken as the basis for an investment decision. The user assumes the entire risk of any use made of this information. The information is provided merely complementary and does not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind. The views expressed therein are based solely on information available publicly/internal data/other reliable sources believed to be true. This report includes projections, forecasts and other predictive statements which represent Crypto.com's assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. Opinions expressed therein are our current opinion as of the date appearing on the report only.

No representations or warranties have been made to the recipient as to the accuracy or completeness of the information, statements, opinions or matters (express or implied) arising out of, contained in or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions contained in this report or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

The reports are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of Crypto.com in any form is prohibited except with the written permission of Crypto.com. Persons into whose possession the reports may come are required to observe these restrictions.

Content

Executive Summary

Welcome to our article on Ethereum's layer two solutions. In this article, we will go through the three types of layer two scaling solutions that have emerged as clear winners in the quest for scalability – sidechains, optimistic rollups, and ZK rollups.

Key Takeaways

- Although they are not a true layer two solution, sidechains are the simplest scaling solution. A sidechain is a separate, more scalable blockchain that operates alongside the main chain. Although they achieve scalability, they do not benefit from the security of the main chain.
- Rollups are true layer two scaling solutions that operate on the back of the main blockchain. They achieve scalability by batching multiple transactions, while applying compression techniques to strip out non-essential data to save block space. Computations for transactions are also moved off-chain, leaving only essential data to be stored on the main chain.
- There are two main types of rollups: optimistic rollups and zero-knowledge rollups (ZK rollups), which differ in how they deal with invalid and fraudulent transactions.
- All of these solutions can achieve transactions per second in the range of 2,000 to 7,000+, more than 100x faster than Ethereum's current fifteen TPS.
- Sidechains and optimistic rollups have significant disadvantages, in contrast to ZK rollups that achieve scalability without sacrificing much.

Introduction

Ever since the inception of Ethereum, scalability has been in the forefront of developers' minds. From the very beginning, it was understood that 15 transactions per second would be insufficient to support a large ecosystem of thousands of applications with billions of dollars of value changing hands every day.

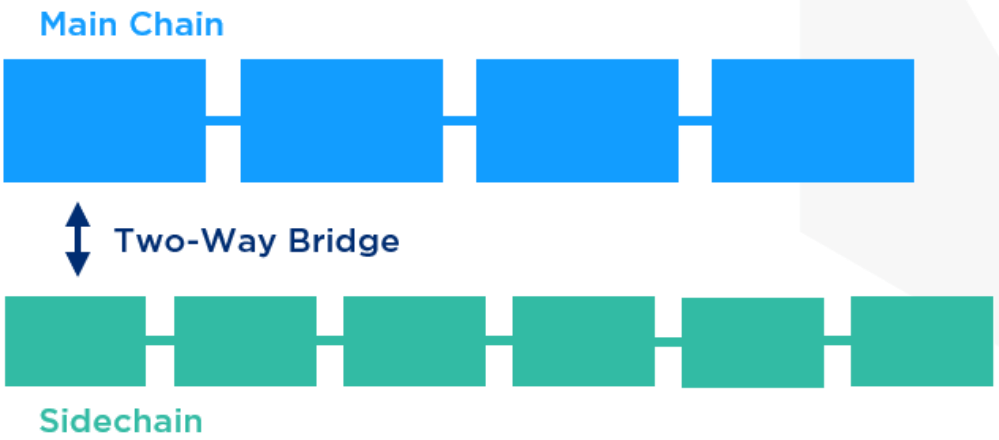
As early as 2017, a mere two years after the launch of Ethereum, Vitalik Buterin and Joseph Poon were already researching layer two scaling solutions in their paper Plasma: Scalable Autonomous Smart Contracts. Since then, developers have been working on numerous other approaches to scale Ethereum, including sidechains, state channels, optimistic rollups, and zero knowledge proof rollups (ZK rollups).

In this article, we will go through the three types of layer two scaling solutions that have emerged as clear winners in the quest for scalability – sidechains, optimistic rollups, and ZK rollups. Don't worry, we will try to keep it simple so that you can understand what layer two is all about!

Sidechains

Examples: Polygon (MATIC), xDai (XDAI)

The simpliest layer two scaling solution are sidechains. As the name implies, a sidechain is a separate, more scalable blockchain that operates alongside the main chain, which in this case is the Ethereum network. The diagram below shows the general principle of how sidechains work:



Transactions occurring on the sidechain don't take up any block space on the main chain, and at the end of it all, users can use bridges to move their assets back onto the main chain.

Although sidechains built on proof-of-stake or other consensus algorithms can improve scalability, it comes with tradeoffs. Since sidechains are essentially a separate blockchain, they don't really benefit from the security of the main chain, which usually has a more diverse set of validators, and a proven consensus mechanism. Furthermore, bridges can be slow and inefficient, leading to long lead times when moving assets between the main chain and sidechain. The bridge itself could also be compromised, preventing users from withdrawing their assets from the sidechain. For this reason, sidechains are not considered by many in the Ethereum community as true layer two scaling solutions.

Rollups

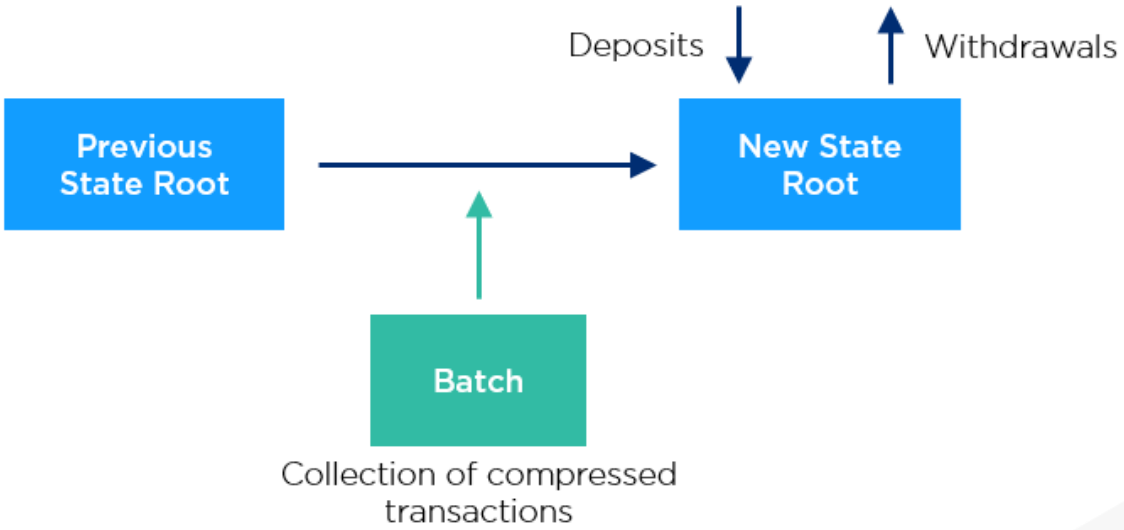
We've gone through some of the benefits and disadvantages of sidechains, which sacrifice security and usability for scalability. The ultimate goal of layer two scaling, however is to maintain the security and capabilities of Ethereum while being fast and inexpensive. This is where rollups come in.

Rollups combine multiple transactions and fit them into a single block, allowing each block to effectively process more transactions. This reduces costs and latency greatly – Vitalik Buterin has stated that transaction speeds could increase by a factor of 100 with rollups.

How do Rollups Work?

Rollups move on-chain storage and computation off-chain but keep just the essential data on-chain. This is achieved by combining multiple transactions, while using superior encoding and data compression to limit the amount of memory that a transaction takes up within each block.

The following diagram is a simplified, generalized demonstration of how rollups works:



A **state root** is a smart contract living on the main chain that represents the state of the rollup – account balances, contract codes, and so on. Operators processing rollup transactions can publish a **batch**, a collection of highly compressed transactions. The contract checks that the previous state root submitted by the batch publisher matches the previous state root, after which the state root is updated to its new state. Any deposits and withdrawals are also processed, with assets flowing in and out of the state root contract as needed.

In this way, rollups can save a significant amount of space that would otherwise have taken up block space on the main chain. You may have noticed, however, that since anyone can publish a batch, this creates incentives for malicious batch publishers to publish fraudulent transactions to steal user assets. How do rollups prevent this? There are two solutions – optimistic and zero-knowledge rollups (ZK rollups).

Optimistic Rollups

Optimistic rollups use fraud proofs to prevent malicious actors from publishing fraudulent batches. The rollup keeps track of the entire history of state roots, which allows transactions to be reverted if anyone discovers an invalid transactions inside of any batch and publishes a fraud proof.

If fraudulent batches are found, the operator responsible will have their staked assets slashed, while the party finding this proof is rewarded with a portion of these confiscated assets.

This mechanism is where optimistic rollups derive their name – it assumes that batches are valid unless proven otherwise. In this way, optimistic rollups can achieve significant scalability for the main chain with 200-2,000 transactions per second versus Ethereum's 15.

There are significant drawbacks, however. Due to its reliance on fraud proofs, withdrawals from optimistic rollups must be subject to a significant delay in order to prevent assets from being withdrawn due to invalid or fraudulent transactions. As long as there is a delay, there will be time to revert transactions in the optimistic rollup.

Optimism is developing optimistic rollups. According to their roadmap, mainnet is due to be launched in July 2021. Many DeFi protocols are already expected to implement Optimism when it launches, including Chainlink, Uniswap, Maker, Synthetix, and Compound.

For a more in-depth look into this scaling solution, you can check out these helpful resources on Optimism's webpage.

ZK Rollups

ZK Rollups, or zero-knowledge proof rollups, take a more conservative route in making sure transactions are valid. It does this by requiring cryptographic proof called a ZK-SNARK (see: PLONK Protocol) to be submitted along with each batch. These proofs can be quickly verified by observers on-chain, leading to greater security and low withdrawal delays since it is virtually impossible for batches to contain invalid transactions. The main players developing ZK rollup solutions are Matter Labs (zkSync), and Starkware.

Comparing Layer Two Solutions

In this section, we summarize the above sections, examining the solutions' benefits and drawbacks against one another.

	Sidechains	Optimistic Rollups	ZK Rollups
Example	Polygon	Optimism	zkSync
Transactions per Second	7,000+	2,000+	2,000+
Benefits	High TPS	High TPS Security of main chain	High TPS Security of main chain Instantaneous withdrawals
Disadvantages	Potentially lower security due to reliance on bridge	Very long withdrawal delays	Technically more challenging to implement due to complex technology

As you can see, all of these solutions offer much higher throughput than the Ethereum network. Although sidechains and optimistic rollups have significant disadvantages that could potentially make them cumbersome to use, they are easy to roll out and operate.

ZK rollups seem to have limited disadvantages – however, the cryptographic proofs that ZK rollups rely on are technologically complex and are very new. Once the technology improves, however, ZK rollups could prove themselves to be the superior layer two solution.

References

Buterin, V. (2021). *An Incomplete Guide to Rollups*. Retrieved from https://vitalik.ca/general/2021/01/05/rollup.html

Ivan on Tech. (2021). *Comparing Layer-2 Ethereum Scaling Solutions*. Retrieved from https://academy.ivanontech.com/blog/comparing-layer-2-ethereum-scaling-solutions

Konstantopoulos, G. (2021). *How does Optimism's Rollup really work?* Retrieved from https://research.paradigm.xyz/optimism

Matter Labs. (n.d.). *zkSync.* Retrieved from https://zksync.io/

Optimism. (n.d.). Retrieved from https://optimism.io/

Polygon. (n.d.). Retrieved from https://polygon.technology/

xDai. (n.d.). Retrieved from https://www.xdaichain.com/

crypto.com

e. contact@crypto.com