The different layer-2 solutions for Ethereum

> 🔗 点击查看原网页
>
> ⏰ 剪存时间：2022-01-08 15:53:52
>
> ✂ 本文档由 飞书剪存 一键生成

Blockchains like Ethereum promise the money of the internet, the world computer, the future of finance (DeFi), the metaverse, and more. However, due to their decentralized architecture, high usage often leads to absurd transaction costs. Layer-2 solutions attempt to overcome these scaling problems.

In the interplay between theblockchain trilemma, chains can usually achieve two of the three properties scalability, decentralisation and security. For a given security level, scalability is inversely proportional to decentralisation. Hence, a blockchain must make trade-offs. On the most prominent blockchain Ethereum, users are negatively impacted by high transaction fees and long waiting times. By processing transactions on a second layer, some solutions try to solve this inherent problem. There are five types of approaches used to deploy layer-2 solutions.

State channels

State channel solutions allow users to transact multiple times on a different chain (layer-2). In contrast, the main chain (layer-1) processes only two transactions, one when the channel is opened and one when the channel is closed. By doing this, the main chain does not process all the transactions but still provides the same level of security in transaction finality. Once the transactions are complete and the channel is no longer required, the participants submit their copies of transaction history to cross-verify their copies of data to ensure there are no discrepancies. Post this, the final net transaction is uploaded on-chain, and the channel is closed.

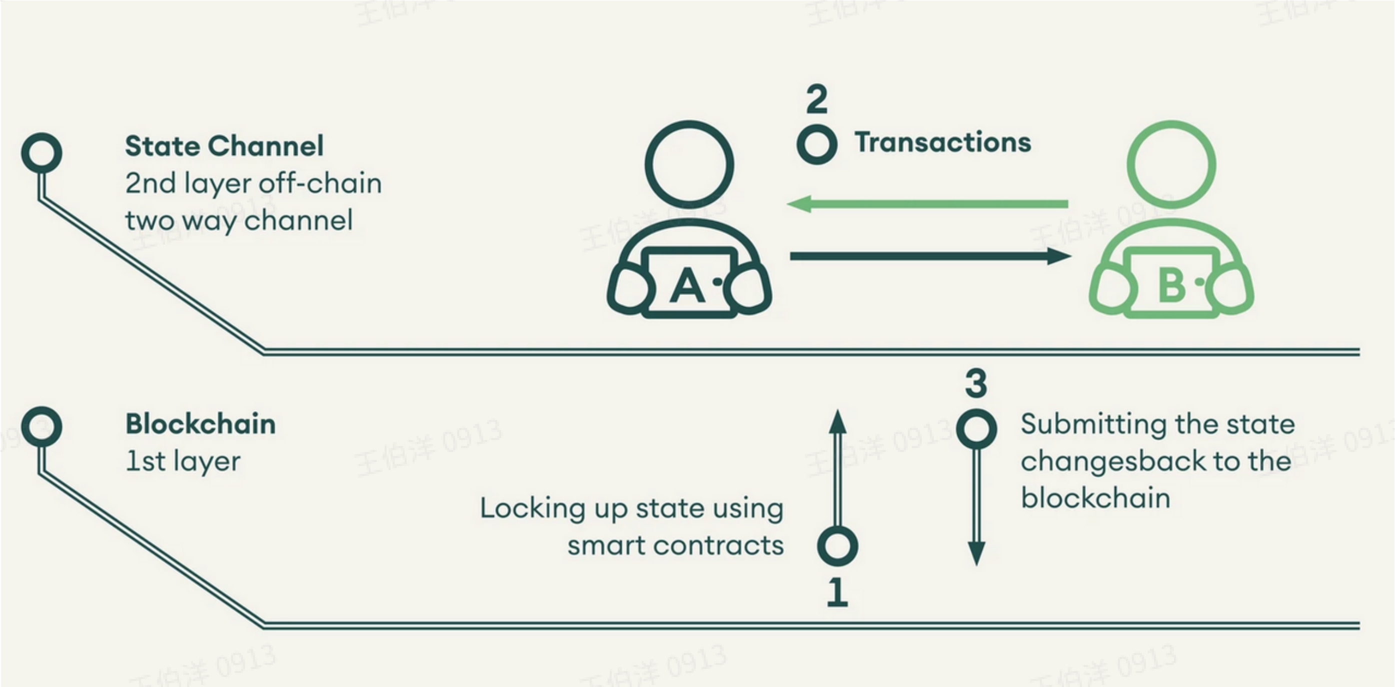


Figure 1 State channel and the steps involved in doing a transaction / Source: SEBA Bank

State channels are advantageous when there are multiple small transactions and the parties know each other. The limitations of State channels are that funds are blocked as long as the channels are active. It is also time-consuming to open and monitor different channels. Further, only limited smart contract functionality is available. Projects working on State channel include Celer and Raiden Network.

Plasma (Child chains)

Plasma consists of multiple copies of the main chain running alongside it. Thousands of transactions are processed in these child chains, bundled up and sent back to the main chain as a single transaction. By definition, a child chain is a trustless and non-custodial chain where users control their funds. Hence if there are any errors or exploits, they can refer to the latest correct snapshots of the plasma chain and restore their tokens.

The advantage of plasma layers is their high throughput to process over 1,000 transactions per second at a fraction of the cost. Here, one necessarily does not need to have a fixed number of known entities or individuals to transact with, and they can be flexible. Like state channels, plasma solutions do not fully support smart contracts and are suitable only for transactions and swaps. Projects that use plasma layers include Polygon and OMG Network.

Sidechains

Sidechains and child chains (plasma) are similar except for one element: security. While plasma chains rely on the security of their main chain in a trustless environment and are optimised for high throughput performance and security, side chains are separate blockchains running in parallel with the main chain and have their own consensus mechanisms and security algorithms.

The advantage of sidechains is that they are usually blockchain agnostic and can support multiple base layers by creating a peg with any blockchain they want to run along. These side chains may have their own tokens, can support smart contracts, and only communicate with the mainchain when they want to update the state of their ledger. These side chains can achieve up to 10,000 transactions per second depending upon their design. However, this also does not come without its disadvantages. Users have to transfer the custody of funds to the side chain, and the security mechanism of the sidechain may be weaker than the main chain. xDai and Polygon are two examples for Ethereum sidechains.

Rollups

Rollups bundle thousands of transactions into a single rollup block, publishing only summary data on the main chain. It can potentially provide a 100x increase in throughput as all the computation and storage happens outside the main chain. By batching transactions and moving processing off-chain, rollups significantly reduce transaction fees and processing time. There are two types of rollups:

Optimistic Rollups

Optimistic rollups use a sidechain to process a batch of transactions parallel to the Ethereum mainchain, summarise it and notarise the transactions on top of the mainnet. They work with a basic assumption that all transactions submitted to the mainchain are valid. Only when a user challenges a summary, the entire block is computed on the base layer. As a result, to give sufficient time for a challenge, funds are locked for some time, typically one week, before releasing them on the base layer.

Optimistic rollups can process around 2,000 basic transfers per second or around 300 smart contract calls in their current implementation. These are also compatible with the Ethereum Virtual Machine (EVM). This means that optimistic rollups can do everything that Ethereum does. However, there are two trade-offs. First, the funds are at risk if a malicious transaction is not challenged and second, withdrawing funds to the mainchain is also time-consuming. Examples of rollups are Optimism and Arbitrum. These projects are already live, and popular projects like Uniswap, 1inch, and Chainlink, among others, are already using them to save transaction costs for users.

Zero-Knowledge (ZK) Rollups

ZK Rollups run all computations off-chain and submit a validity proof on Ethereum. They differ from optimistic rollups because there is no trust assumption as the validity proof is printed on-chain. While optimistic rollups require evidence of fraud during the challenge, zk rollups have validity proofs for every transaction.

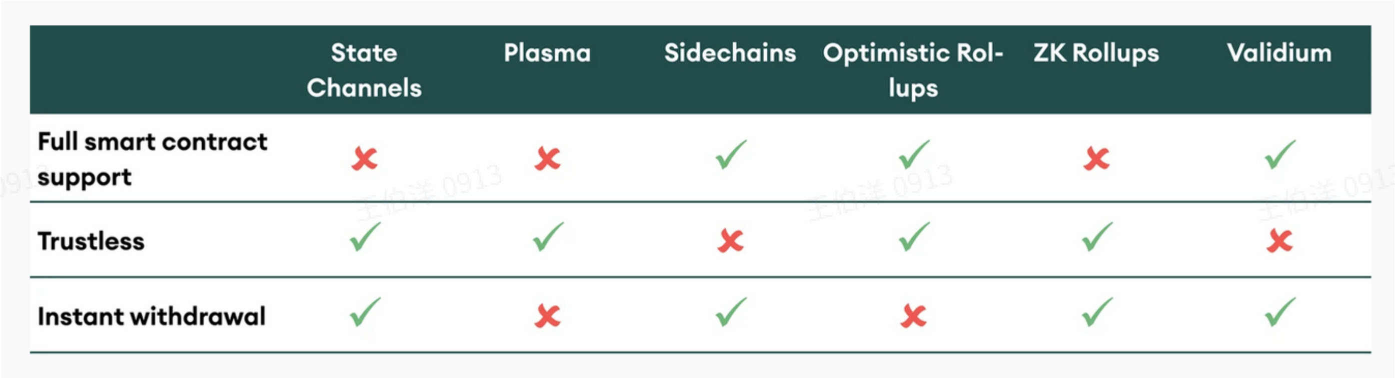
They are reported to be able to process over 3,000 transactions per second on Ethereum. As there is no trust assumption, there is no delay in moving funds from layer-1 to layer-2 and vice versa. Currently, there is no generalised EVM-compatible zk rollup based solution, and only specific solutions for transfer or exchanges are available. Loopring is a decentralised exchange working on zk rollups with transaction costs of less than a cent.

Validium

Validium uses validity proofs similar to zk rollups but keeps the data off-chain instead of sending it to the Ethereum main chain. Since all the data is kept off-chain, Validium can achieve an even higher TPS per validium chain of up to 20,000. However, since the data is not on-chain, validium requires some trust assumptions, and a majority of validators can choose to freeze funds by not providing data. StarkWare’s StarkEx is a validium-based solution. StarkEx is integrated with the derivatives exchange, dYdX, and the NFT platform, ImmutableX.

Conclusion

For blockchains and crypto assets to achieve their lofty promises of world computers and money for the internet, they must be able to scale sustainably. For this, a combination of both layer-1 and layer-2 solutions will be required. Currently, chains are sacrificing decentralisation to achieve scalability, or a hotchpotch of solutions are being implemented with limited integrations between them, worsening the user experience and fragmenting the user base.



	State Channels	Plasma	Sidechains	Optimistic Rollups	ZK Rollups	Validium
Full smart contract support	✗	✗	✓	✓	✗	✓
Trustless	✓	✓	✗	✓	✓	✗
Instant withdrawal	✓	✗	✓	✗	✓	✓

Figure 2 Comparison between different layer-2 solutions and the trade-offs they make / Source: Matter Labs, SEBA Bank

Solving scalability will not be a winner-take-all scenario, and different use-cases will require different scaling and security needs. Improvements in scalability from layer-1 and layer-2 solutions will multiply in the future, leading to sustainable, scalable blockchains.