Hex Trust

Blockchain Scaling

An overview of how blockchain scaling technology has evolved over the years

Hex Trust Insights

February 2023

Contents

Introduction

The blockchain market has achieved tremendous growth in a relatively short amount of time, far outpacing the adoption rates of other technologies and their applications such as the internet, smartphones and social media. However, mainstream adoption still remains a challenge due to the prevalent issues around security, transparency, and scalability. As the demand on blockchain systems grows, scalability issues in particular need to be addressed in order to maintain the speeds that meet the needs of a broader retail user base.

Some of the most widely used blockchains such as Bitcoin and Ethereum have received criticism in the past for the networks' increasingly high cost and slow transaction speeds, unable to offer appropriate entry points for widespread retail use. In particular, such networks have been facing congestion issues, failing to keep up with the increasing number of transactions that inevitably come with growing fame.

Addressing these issues, developers in the digital asset ecosystem are continuously working towards improving the infrastructure that supports the decentralized economy. There have been many solutions to such congestion issues: the Ethereum Merge for example, which took place September 2022, was one of those initiatives.

There is an entire sector within the digital asset industry of projects dedicated to alleviating blockchain congestion – with one famous example being Polygon. These projects are often referred to as scaling solutions.

What is Blockchain Scaling Technology?

Blockchain scaling technology helps keep the blockchain functioning as expected, with respect to the number of transactions processed in a certain period of time even as network usage increases. Components of scalability are blocktime and size, transaction speed and volume, and cost per transaction.

For blockchains like Ethereum to become the ultimate programmable base settlement layer, they must be capable of competing with the likes of traditional finance juggernauts like Mastercard and Visa, which process up to 24,000 transactions per second. Amongst others include being able to host many more validator nodes and being free from security threats. Although not all of these factors are tackled by blockchain scaling technology, it plays a critical role in unlocking the next growth chapter for the digital asset industry.

Important Terminologies

State:

All available information about a network at a specific point in time. A state can encompass a chain's present condition and specified details such as accounts, balances and smart contracts.

State root:

A cryptographic commitment verifying a chain's status at different points in time.

State transitions:

Transactions made on the blockchain which cause a state change to the network's state root.

Merkle tree:

A mathematical data structure made up of hashes of various data blocks summarizing all transactions in the block. Enables quick and secure content verification across large datasets.

Merkle root:

A simple mathematical method for confirming information on a Merkle tree. Allows verification of whether specific pieces of data is part of a large data set and ensures data blocks sent through a peer-to-peer network are whole, undamaged and unchanged.

Fraud proof:

A claim that a state transition is invalid and the entire batch of transactions should be reverted.

Validity proof:

Provides cryptographic certainty that state transitions to main chains are correct.

Zero-Knowledge Proofs:

A cryptographic method to prove one party (the prover) can prove to another party (the verifier) that a given statement is true without revealing the statement itself.

The Evolution of Blockchain Scaling Technology

At the core of blockchain technology lies decentralization, which plays a big role in the growth of the entire digital asset industry. More users are looking to leverage the increased control of their assets, access to true ownership rights, and global connectivity that decentralized technology has to offer.

Decentralization is a fundamental principle for all projects in the Web3 space. For blockchains to be truly decentralized, they must accommodate a higher number of computers to participate in securing the network. To do so, the network must keep its core protocol requirements very light, lowering the barrier of entry for those wanting to participate.

One of the goals of blockchain scaling technology is to increase the rate of blockchains' data processing while maintaining low requirements for nodes to participate in the network. This is what will help blockchains reach sufficient degrees of decentralization.

There are four primary used scaling solutions: state channels, plasma, optimistic rollups and ZK-rollups.

State Channels

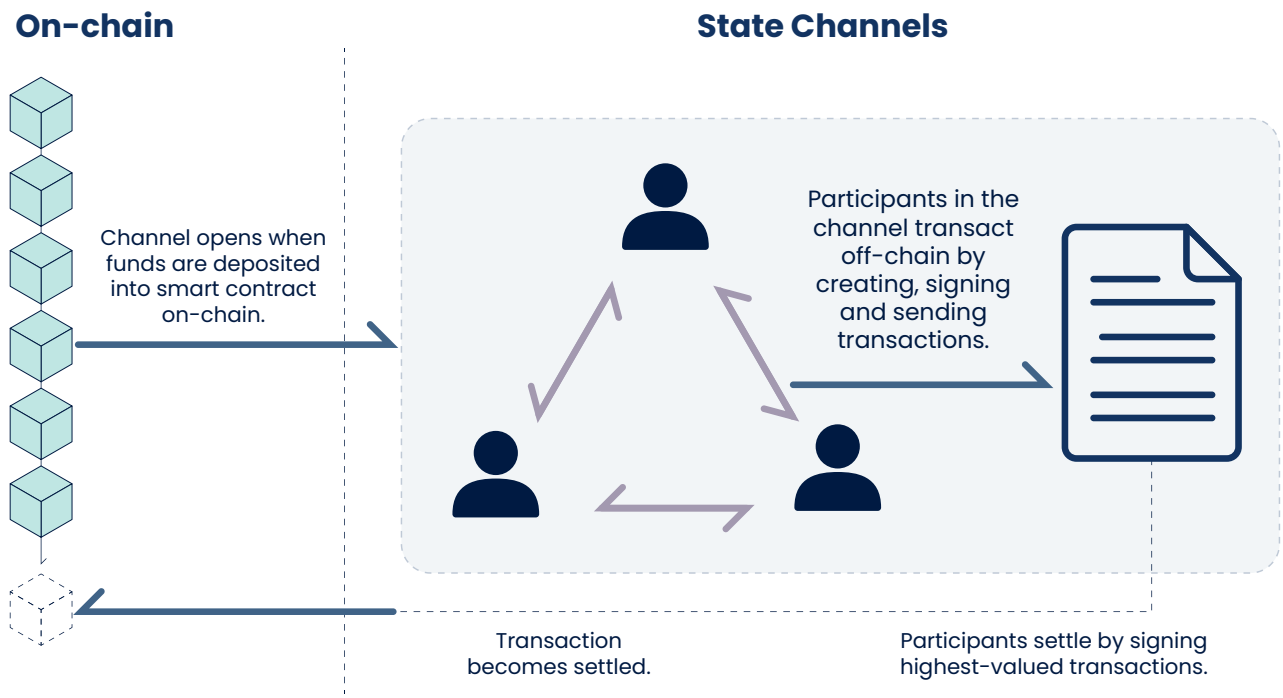
What is it?

State channels are the very first type of blockchain scaling solution that emerged to address blockchain congestion. It reduces strain on the main chain by allowing users to transact off-chain. Within state channels, users can conduct an arbitrary number of transactions off-chain while only needing to submit two transactions on-chain.

How does it work?

For a state channel to be opened, a user must first deposit their funds into a smart contract on-chain. This will put the funds in escrow, meaning they cannot be touched until the channel is closed. Once the user is in the channel, they will be able to make transactions with one another for little to no cost. Users will then be required to sign a ticket which sends an off-chain message to the receiver. In the channel, users are able to conduct an arbitrary number of transactions or payments.

Once the transactions are completed, users sign and publish the highest-valued transaction back on-chain to the blockchain network. The on-chain smart contract will then verify that transaction, and settle the state channel by unlocking the funds in escrow. If one participant does not agree to the settlement, they are able to initiate a withdrawal period.



Example: Lightning Network

Lightning Network is a layer-2 network designed to support the Bitcoin blockchain. Bitcoin was initially designed as a simple decentralized payment system and was not able to accommodate scalability. Lightning Network is the layer that helps the Bitcoin network scale its capacity and conduct transactions more efficiently using payment channels. This allows users to make payments with one another in a cheaper, faster, and more readily confirmed way. The network can also be used to conduct other types of off-chain transactions that involve the exchange of Bitcoin.

Although payment channels are not the same as state channels, they are very similar in nature. Payment channels are merely one type of state channel, and its distinctive feature is that it only supports payments rather than general state changes.

Limitations

Although state channels improve congestion issues on blockchains, it comes with its fair share of limitations. State channels put restrictions on who is able to conduct the transactions – meaning, users are unable to send funds off-chain unless they're a participant of a specific channel. Plus, a large amount of capital needs to be locked in order to make use of state channels.

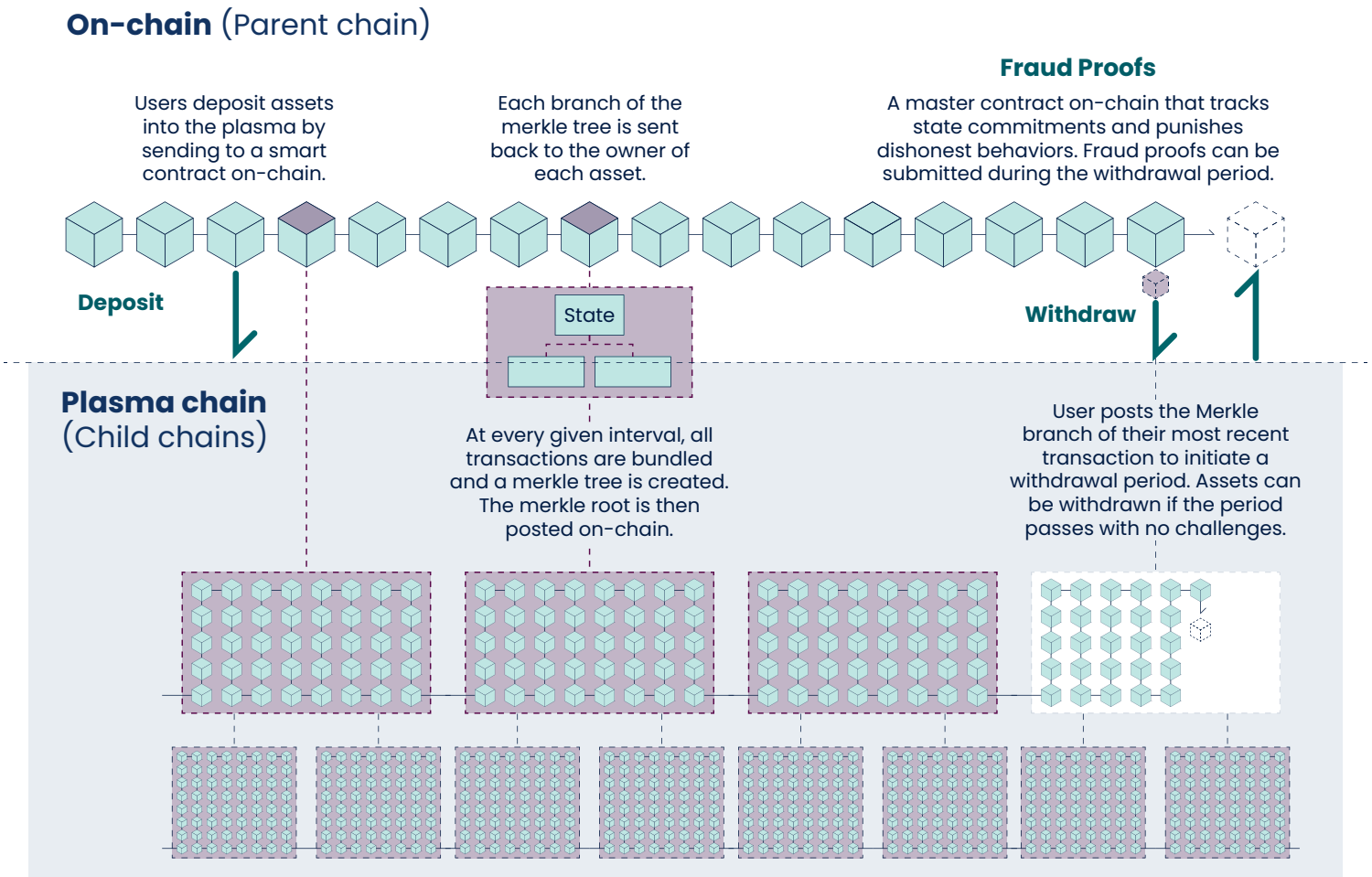
Due to such limitations, state channels are mainly used by niche applications or chains that are unable to support more modern scaling solutions.

Plasma chains

What is it?

Plasma was introduced as a scaling solution addressing the limitations of state channels. Plasma is similar to state channels in that they both move the transaction load off the mainnet as much as possible.

The plasma structure is essentially a framework which enables the creation of unlimited child chains that each have their own independent state and virtual machine. They operate via their own consensus mechanism and store all relevant data including accounts, smart contracts and balances. They make use of Merkle trees to organize states, which reduces the data to a single hash. This enables efficient data confirmation on the blockchain without requiring the entire dataset.



How does it work?

Users must first deposit funds to the smart contract on-chain in order to open a Plasma. In return, the plasma smart contract mints an equivalent amount of assets on the Plasma, which is then sent to the depositor. Similar to state channels, the deposited funds go in escrow and will only become available again once the transaction is completed.

The child chains are essentially copies of the main chain which is used as an arbitration layer. Each child chain can be configured in terms of consensus mechanism, block sizes, confirmation times and more, to match the needs of a specific use case. So, an individual child chain operates independently while co-existing with other child chains. More chains can be built on top of each child chain as well, which is where the Merkle tree organization function comes into play.

So when a user deposits their funds, it enters an independently operating, highly centralized plasma chain. The plasma chain periodically (e.g. every 15 seconds) posts the state root, so at every interval, the received transactions are bundled into groups and a Merkle tree for the state of the plasma chain is generated. This plasma operator then posts the Merkle state root (a single hash representing the required data) to the main chain. Each Merkle branch (a specific requested transaction) is then sent to the respective owner of a particular asset.

Deposits and withdrawals of funds in plasma chains, which are state transitions, can be enabled by something called fraud proofs. Fraud proofs are a master contract on-chain that tracks state commitments, and punishes any dishonest behaviors. They are responsible for ensuring that in the case of malicious acts, participants can report dishonest nodes, protect their funds, and exit a transaction. Simply put, fraud proofs are the mechanism for which a plasma child chain files a complaint to the main chain.

To do so, fraud proofs use an interactive-withdrawal protocol. When a user wishes to withdraw a certain amount, they initiate a withdrawal period. The withdrawer confirms the details of the withdrawal, and other participants then submit a Merkle branch which has been confirmed and tested if any funds were spent. If the event seems wrong, any participant can submit a Merkle branch proving the withdrawer doesn't own the respective funds, and the event is then considered fraudulent and canceled. If the withdrawal period passes without challenges, the withdrawal will be successful.

Example: Polygon (Matic Network)

Polygon Technology, originally launched as Matic Network in 2017, is currently the most widely used scaling solution. It is designed to support the Ethereum network with scalability, and has already established itself as the most promising scalability project with a strong developer team.

When Matic Network launched, it had one primary offering: Plasma chains. The network's plasma chains ran independently with their own Proof-of-Stake consensus mechanism. They help move transactions off-chain from Ethereum, overall alleviating the network's congestion issues while uncompromising on security. Plasma chains are still offered with Polygon despite the name change, and continue to be one of the main options for developers to integrate with the blockchain.

Improvements & Limitations

Plasma chains provide several improvements to state channels. To start off, there are no strict participation requirements like with state channels, meaning non-participants of a channel can also contribute. Plasma chains also support a persistent state (as they exist in their own context), whereas state channels are newly created and destroyed each time a user wishes to transact off-chain. Lastly, Plasma introduces improved network security as records of transactions are always available on-chain during operations, and chains can be quickly exited by participants.

However, using plasma chains does come with its own set of trade-offs. The main trade-off is higher cost - using plasma chains require regular transactions on the main chain. In the scenario where a sufficiently large amount of users are wishing to withdraw at once, it can also lead to congestion. Additionally, instant withdrawals are not supported as using Plasma requires a withdrawal period of one week. As plasma relies on fraud proofs, the withdrawal period of 7-14 days is given to allow other participants in the plasma chain to potentially submit a proof to challenge the withdrawal.

Despite the fact that plasma chains are independent and host their own states, they are unable to host full EVM environments. This poses a challenge for applications that require explicit consent from owners. Most importantly, plasma chains lack data availability which means transaction data in a block is not easily available to all participants. With only the Merkle root sent back to the mainnet, users cannot conduct withdrawals if the plasma operator were to stop sending fraud proofs.

Plasma chains are still used frequently in blockchain applications and will continue to be of great contribution to scaling.

Optimistic rollups

What is it?

Optimistic rollups were introduced as a way to address the data availability issue of plasma chains – instead of just sending back the Merkle root to the main chain, optimistic rollups put all data on-chain to locally process operations.

Optimistic rollups are just another way to reduce the load on main chains and conduct transactions off-chain for improved efficiency. Its distinctive feature is that it assumes no malicious actors are involved, and all participants maintain their integrity through economic incentives - hence, the optimism. They are called "rollups" because they 'rollup' thousands of transactions together in batches before sending them back to the main chain.

How does it work?

Optimistic rollups use similar processes to plasma chains, with a few tweaks. There are three main stages of optimistic rollups: entering the rollup, using the rollup, and exiting the rollup.

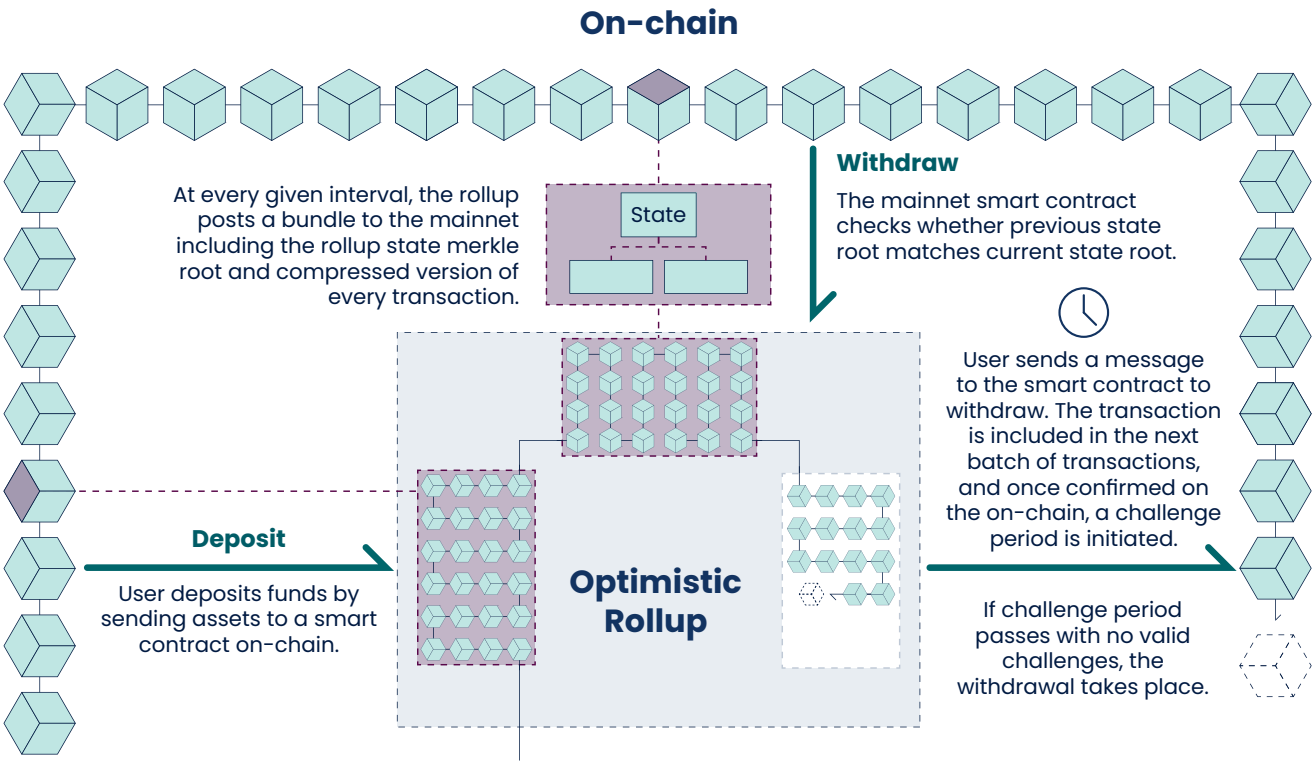
To enter an optimistic rollup, users must first deposit funds into the rollup's smart contract which manages the interaction between the main chain and the side chain. Once the funds are deposited, they are locked up and an equivalent amount of assets are minted on the rollup. A third party known as the sequencer, sends the user the rollup assets once proof of deposit has been received. The user is then free to transact with the rollup assets until their balance is exhausted.

The sequencer also plays an important role in facilitating the use of optimistic rollups. On the rollup, users must sign transactions and submit them to the sequencer, which is responsible for ordering and executing transactions. They first verify the transactions, compress its data into a block, then submit it to the main chain as a single transaction. During the process, the sequencer must submit the transaction along with the state root, including the pre-state root and post-state root.

Here, the pre-state root refers to the old state root which contains information before the transaction is executed, and the post-state root refers to the new state root containing information after the transaction is executed. Once the sequencer submits the batch of transactions, the rollup contract verifies that the pre-state root matches the existing state root. If they match, the contract discards the pre-state root and stores the post-state root as submitted by the sequencer.

Transactions submitted in the post-state root are considered final and irreversible, with no additional proof required. However, if a user wishes to propose a particular transaction is fraudulent, they may do so using a fraud proof (similar to Plasma).

To exit the optimistic rollup or withdraw one's assets, a user must submit a Merkle proof to the rollup contract which proves their specific transaction is part of the rollup's state root. To create a Merkle proof, the user needs access to initial transaction data which the sequencer provides. Once the withdrawal is initiated, the transaction becomes included in the next batch of transactions. Once the batch is published on-chain, a challenge period begins. If the period passes with no valid challenges, the withdrawal is successful.



Example: Arbitrum

Arbitrum is an optimistic rollup project which aims to improve Ethereum's user costs and transaction speed. It does so by utilizing optimistic rollup technology to move data and computation of transactions off-chain, resulting in cheaper and faster transactions. Its Arbitrum Virtual Machine (AVM) supports EVM compatible smart contracts, meaning users can freely use Ethereum-based decentralized applications for a much lower cost.

Improvements & Limitations

Optimistic rollups are a viable way to eliminate the need for explicit ownership. Additionally, rollups are able to run an EVM. It also provides enhanced data availability compared to plasma chains as all transaction batch-related data is posted to the main chain, allowing anyone to reproduce and verify.

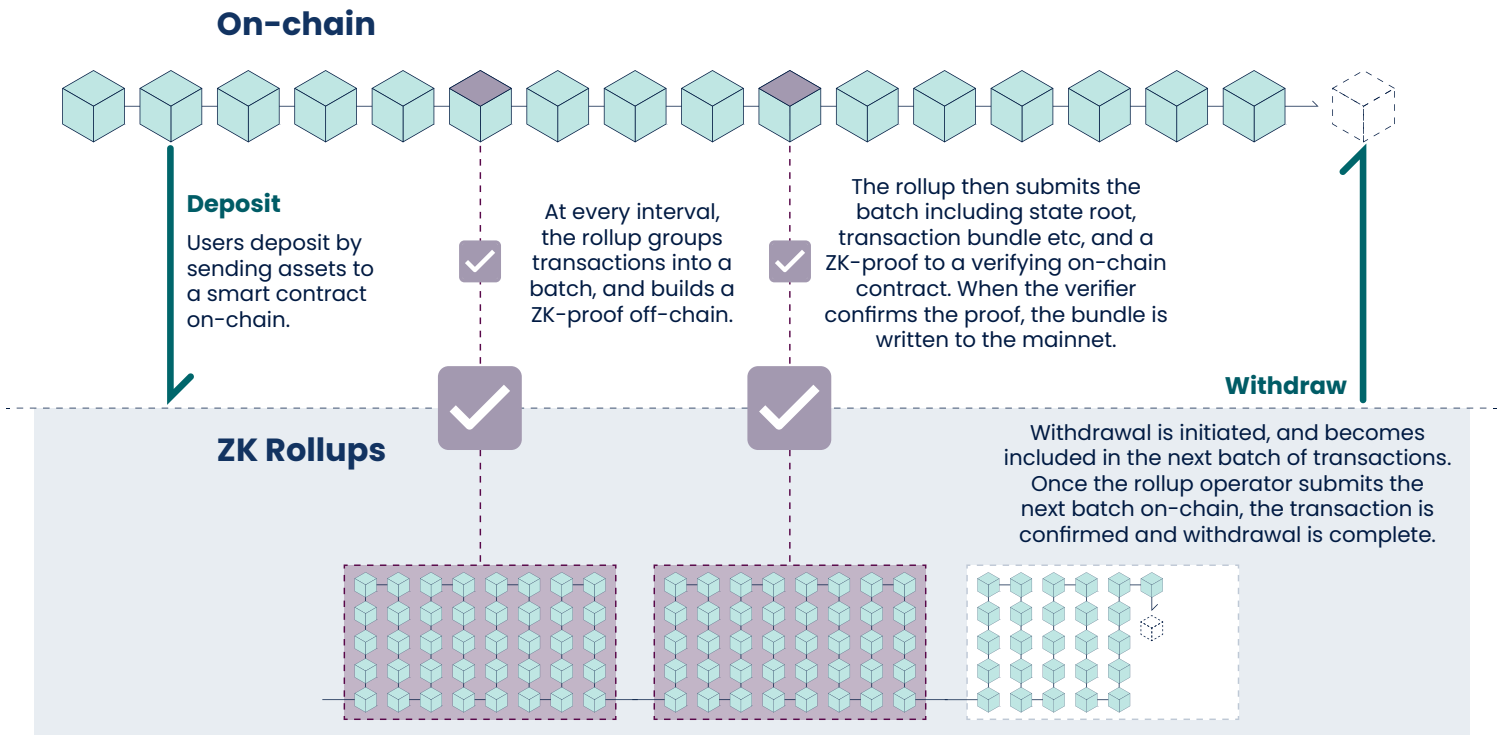
The biggest pain point of optimistic rollups however, is ironically its abundance of optimism. All incoming transactions are considered valid, as it relies on economic incentives of untrusted participants to maintain integrity. Sequencers are fully assumed trustable to identify whether state roots sent back to the main chains are true. Another limitation is similar to struggles of plasma chains: the lack of instant settlements. Lengthy challenge windows have to be passed before settlements are finalized and participants are able to withdraw their assets, making it suboptimal for situations where instant settlements are required.

Zero-Knowledge rollups

What is it?

The most recent version of blockchain scaling technology is Zero-Knowledge Rollups (ZK-rollups). Similar to other blockchain scaling solutions, the goal of ZK-rollups is to increase throughput on the main chain of blockchain networks by moving computation and data off-chain. They are very similar in nature to optimistic rollups, but with another question in mind: how do we finalize transaction batches the moment they are received on-chain?

In a nutshell, ZK-rollups (like optimistic rollups) bundle transactions together to execute them off-chain. By doing so, computation is moved off-chain, reducing the amount of data that has to be posted on the main chain. ZK-rollup operators post a summarized version of changes needed to represent all transactions in batches rather than sending individual ones separately. They also provide something called validity proofs, which are used to verify all the changes made to the state root. Validity proofs show cryptographic certainty that state transitions to main chains are correct.



How does it work?

The way ZK-rollups work is identical to the way optimistic rollups work when entering and using the side-chains. A user first deposits funds into the rollup's smart contract, and the funds are then placed in escrow until the transaction is completed.

But to understand how ZK-rollups work specifically, one must first understand Zero-Knowledge Proofs (ZKPs).

ZKPs are a way to prove that you know something without actually revealing the information. It bundles hundreds of transactions together, compresses them to one single transaction, and sends them back on-chain. This single transaction takes the form of a validity proof. Validity proofs are also known as either a succinct, non-interactive, argument of knowledge (SNARK) or a succinct, transparent, argument of knowledge (STARK). SNARKs and STARKs are similar to cryptographic transaction hashes. Each transaction is identified using a unique transaction hash without revealing any information about the transaction itself.

A fundamental difference of ZK-rollups compared to optimistic rollups is the reduced waiting time when withdrawing assets. Whereas optimistic rollups force a lengthy challenge window to be passed before one can re-access their funds, ZK-rollups do not require such a window. When ZK-SNARKs are sent back to the main chain's smart contract, it verifies if the proof is valid or not on-chain. It takes around 12 seconds for ZK-SNARKs to be processed on-chain, and the withdrawal is then included in the next batch of transactions. Once the rollup operator submits the next batch of transactions, the withdrawal transaction is confirmed and users are able to withdraw their assets.

Example: ImmutableX

Immutable X is a layer-2 blockchain designed to support the Ethereum network's scalability. It allows users to create and manage NFT projects in a secure way with zero transaction costs. It also offers quick trade confirmation, zero gas fees, and large scalability without compromising security.

ImmutableX

Immutable X is able to process up to 9,000 transactions and mints per second using ZK-rollup technology. The use of such technology allows the platform to validate transaction blocks faster, and reduce computation. It also provides ease in moving transactions from layer-2 platforms to layer-1s as validity proofs are generated and approved by ZK-rollup contracts.

Improvements & Limitations

ZK-rollups are a way to eliminate the challenge window needed with optimistic rollups. Users are able to withdraw their assets almost immediately once transactions are completed. They also provide data availability, as the state data of all transactions processed off-chain are published on the main chain. With such data, others are able to reproduce certain rollup states and validate transactions themselves.

However, ZK-rollups do have their own challenges. First off, complex validity proofing: the difficulty in computing knowledge to produce ZPKs may sometimes require data optimization for maximum throughput. There is also the aspect of security concerns, as only one network participant is considered honest to validate rollup data. This points to the possibility of all participants being corrupted. Finally, ZK-rollups do not support smart contract execution. This remains an ongoing issue, which several upcoming projects aim to solve.

Scaling for mass adoption

Blockchains lay the foundation for the permissionless future and an expansive decentralized economy. Use cases have already ventured beyond finance into digital identity, collectibles, metaverse, GameFi, arts, entertainment and so much more, attracting millions of new users.

However, if the foundation is not strong enough to scale in line with an increasing number of users and applications entering the Web3 space, the entire ecosystem is limited in terms of growth. It is crucial for blockchain networks to keep addressing these limitations, and improve scaling technologies in order to achieve the grand vision of having more than a billion users on the blockchain.

HexTrust

Digital Asset Custody
Meets Innovation