Polygon zkEVM:ethereum compatible layer2 scaling solution

==========

1. Introduction

The Ethereum blockchain network has suffered scalability issues over the past few years. In 2017, a game developed on the ethereum network called CryptoKitties became so popular that it took up to 10 percent of network space available for ethereum transactions. The increased traffic led to increased gas costs and a slowing down of transaction executions.

To solve some of the issues of the ethereum network Polygon MATIC was created in India in 2017 by a team of developers and blockchain experts led by Jaynti Kanani and Sandeep Nailwal. Matic Network was rebranded to Polygon in 2021.

2. Polygon PoS (Matic Network): How does it work?

Polygon is a blockchain network that aims to provide a high-performance and low-cost alternative to Ethereum for building decentralized applications (dApps). Polygon works on a proof of stake model, which relies on people staking their tokens and locking them up to be eligible for staking rewards.

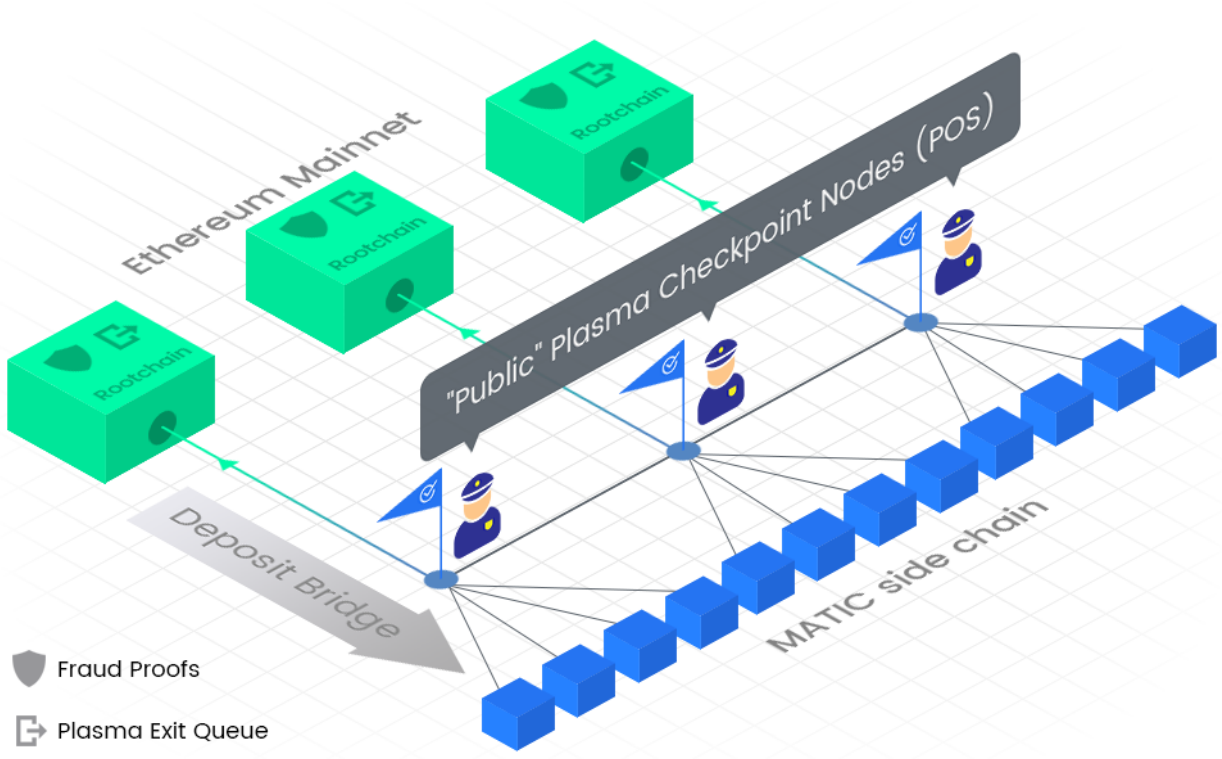
It is built on top of Ethereum using a technology called "Plasma," which enables it to handle higher transaction throughput and lower transaction fees than Ethereum.

3. Sidechains and plasma chains

A side chain is a separate blockchain attached to a main blockchain, allowing for the transfer of assets between the two chains. Sidechains do not rely on the security of the main chain, while Plasma chains' security depends on the main layer.

In contrast to sidechains, however, the “root” of each plasma chain block is published to Ethereum.

Polygon PoS uses an adapted version of Plasma with Proof-of-Stake (PoS) based side chains. It provides a solution for faster and low-cost transactions with finality on the main chain. Verification of the State root, which is **the hash of all the account balances, contract storage, contract code, and account nonces,** enables an added layer of security compared to side chains which do not depend on the mainchain for its security.



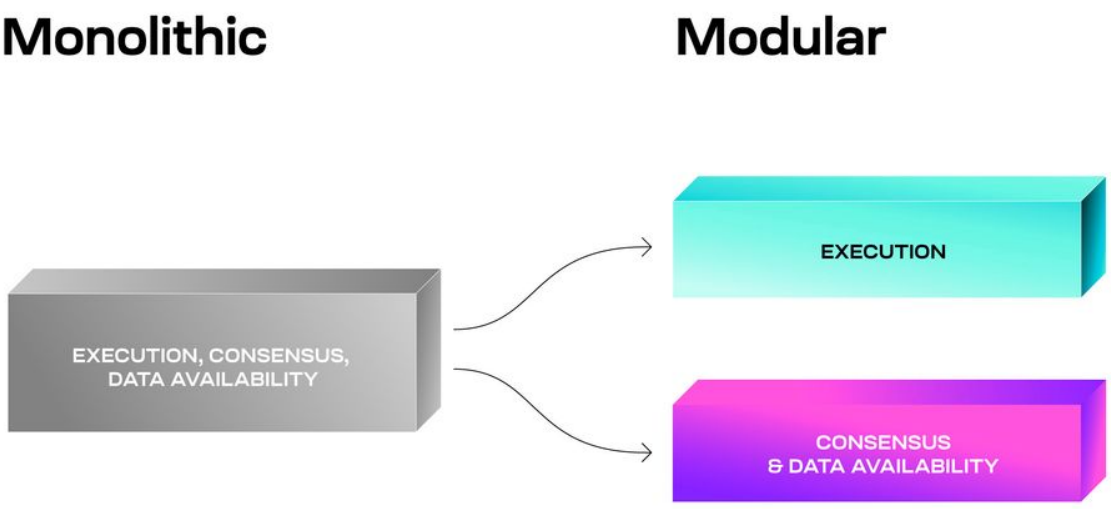
4. Issues with Plasma based chains

Plasma chains record state roots only on-chain, and the transactions executed off-chain are not stored in Ethereum. It results in a "data availability problem" whereby participants in the network cannot access transaction data if there are malicious block producers.

To tackle these issues, Matic rebranded itself as Polygon, and the team decided to focus on various types of rollup networks and modular components.

5. Modular Blockchains and Polygon

Ethereum, Bitcoin, Solana, etc., carry out all four primary functions of the Blockchain, like consensus, settlement, execution, and data availability, on the same layer and are called Monolithic Blockchains.

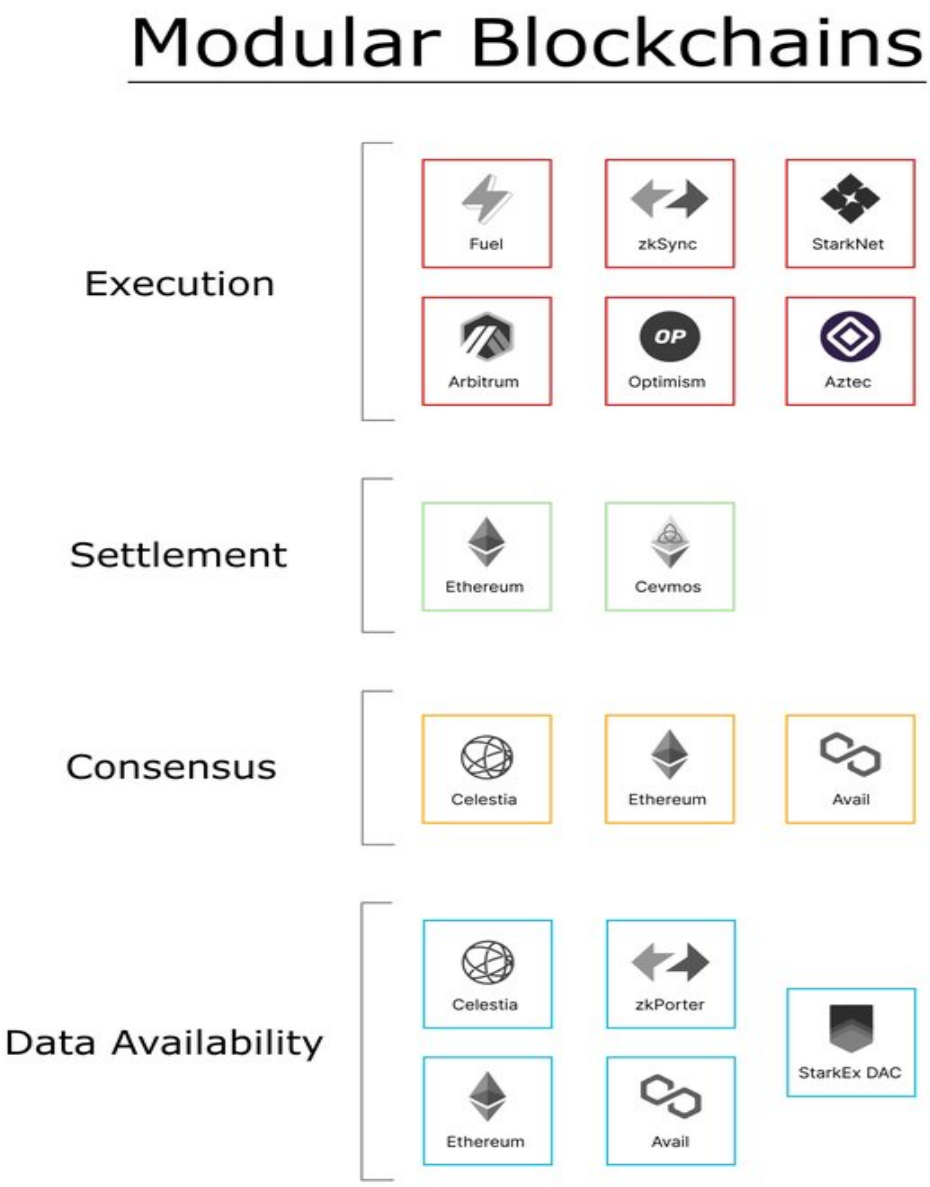


Source: Celestia

A modular blockchain handles a few of these functionalities at the base layer and outsources the remaining functionalities to other layers. Modular Blockchain architecture is proposed to be a solution for Blockchain scalability trilemma as it splits up the blockchain processes among multiple specialized layers.

Some of the modular blockchain products by Polygon are as below:

- **Polygon PoS:** It is the most actively used network.
- **Polygon Avail:** It is a data availability layer that helps execution layers on top of it to store transaction data safely and scalably.
- **Polygon zkEVM:** It is the first ZK-rollup using decentralized sequencers. It will also support Opcode-compatible zkEVM.
- **Polygon Zero:** A ZK-rollup that uses a technology called Plonky2 to generate the fastest recursive proofs.
- **Polygon Miden:** ZK-STARKs-based ZK-rollup.
- **Polygon Nightfall:** Privacy-enabled optimistic rollup.



From the figure, we can see that both Optimistic rollups and zkRollups perform execution off-chain, whereas networks like Celestia, Polygon Avail, etc., perform consensus and data availability off-chain.

6. How Roll ups prevent the data availability problem

Data availability requirement in a Blockchain expects that all transaction data is available on chain at all times. Plasma chains store transaction data off-chain, which can cause data availability problems, whereas in rollups, the transaction data is stored on-chain in Ethereum, preventing the data availability problem.

Rollups collect batches of transactions and does transaction execution off-chain, rolls them up, and sends the transaction data on-chain.

Optimistic rollups and ZK-rollups

Optimistic rollups and ZK rollups are the two main types of rollups. Optimistic rollups use fraud proofs, a Merkle root of the rollup's state, to verify the validity of a state root. However, due to the time set to account for potential fraud challenges, the users have to wait for a one-week challenge period before withdrawing their funds from ethereum.

ZK-rollups use validity proofs(zero-knowledge proof) for instant verification of transactions every time a batch is submitted. The validity proofs are computed off-chain, and the verification is done on the Ethereum network. The sequencer calculates the validity proofs and also determines the transaction order in ZK-rollups.

7. Polygon Hermez 1.0

Zero-knowledge (ZK) proof is a cryptographic technique that helps one party (prover) to prove to another party (verifier) the validity of information without revealing the actual content.

In August 2021, Polygon purchased the ZK-rollup project Hermez network for $250 million of MATIC tokens. Hermez 1.0, which has been live on the mainnet since March 2021, was the first-ever decentralized ZK Rollup on the Ethereum mainnet. Polygon Hermez focused on scaling payments and token transfers on top of Ethereum.

Initially, Hermez only had one product running, an L2 payments platform based on ZK technology called Polygon Hermez 1.0 . Polygon Hermez 1.0 is the first rollup to introduce the Proof of Donation (PoD) consensus mechanism for decentralization.

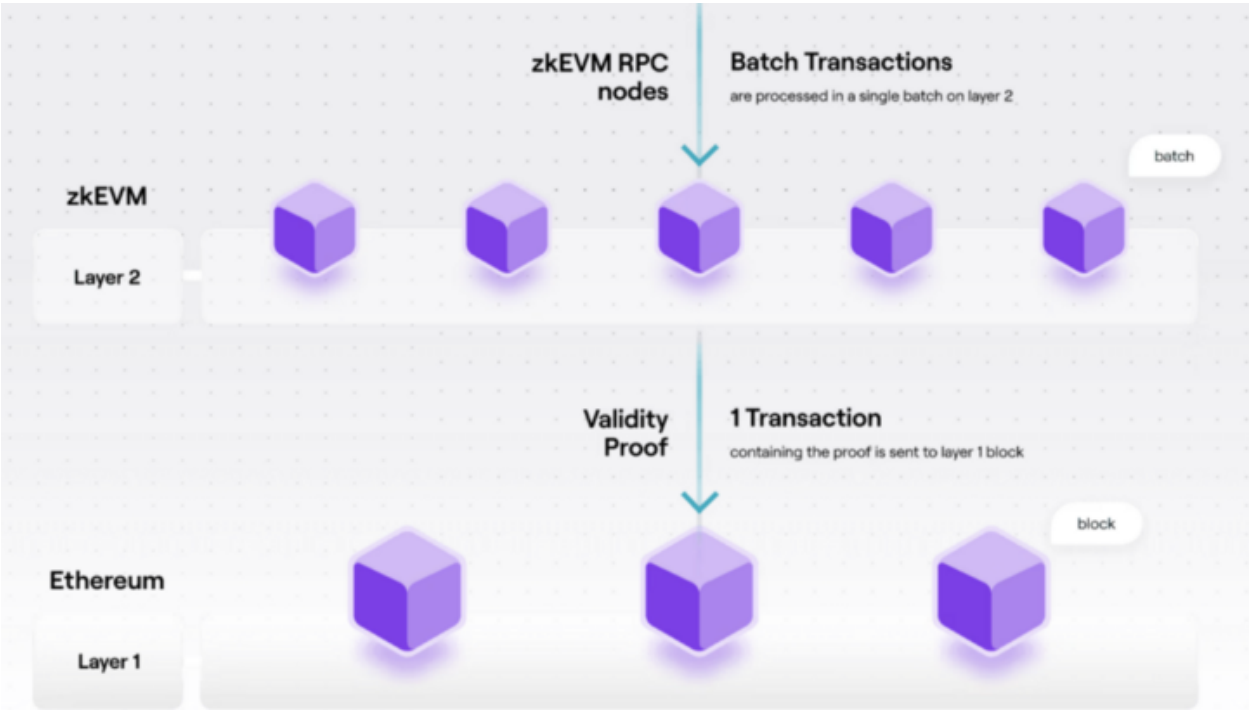
Multiple coordinators coexist in the network running Hermez nodes. The Coordinators receive transaction requests from users, execute them, and submit the state root, transaction data, and zero-knowledge proof to the Ethereum network. They will compete in a decentralized auction process managed by smart contract for the right to publish the block into the network.

After Hermez 1.0, the Polygon Hermez team has come up with the Proof of Efficiency (PoE) model for Polygon zkEVM. Polygon zkEVM, rebranded from Polygon Hermez 2.0, is still under development and the first public testnet launched in October 2021 .

8. Polygon zkEVM- an EVM-compatible ZK-rollup

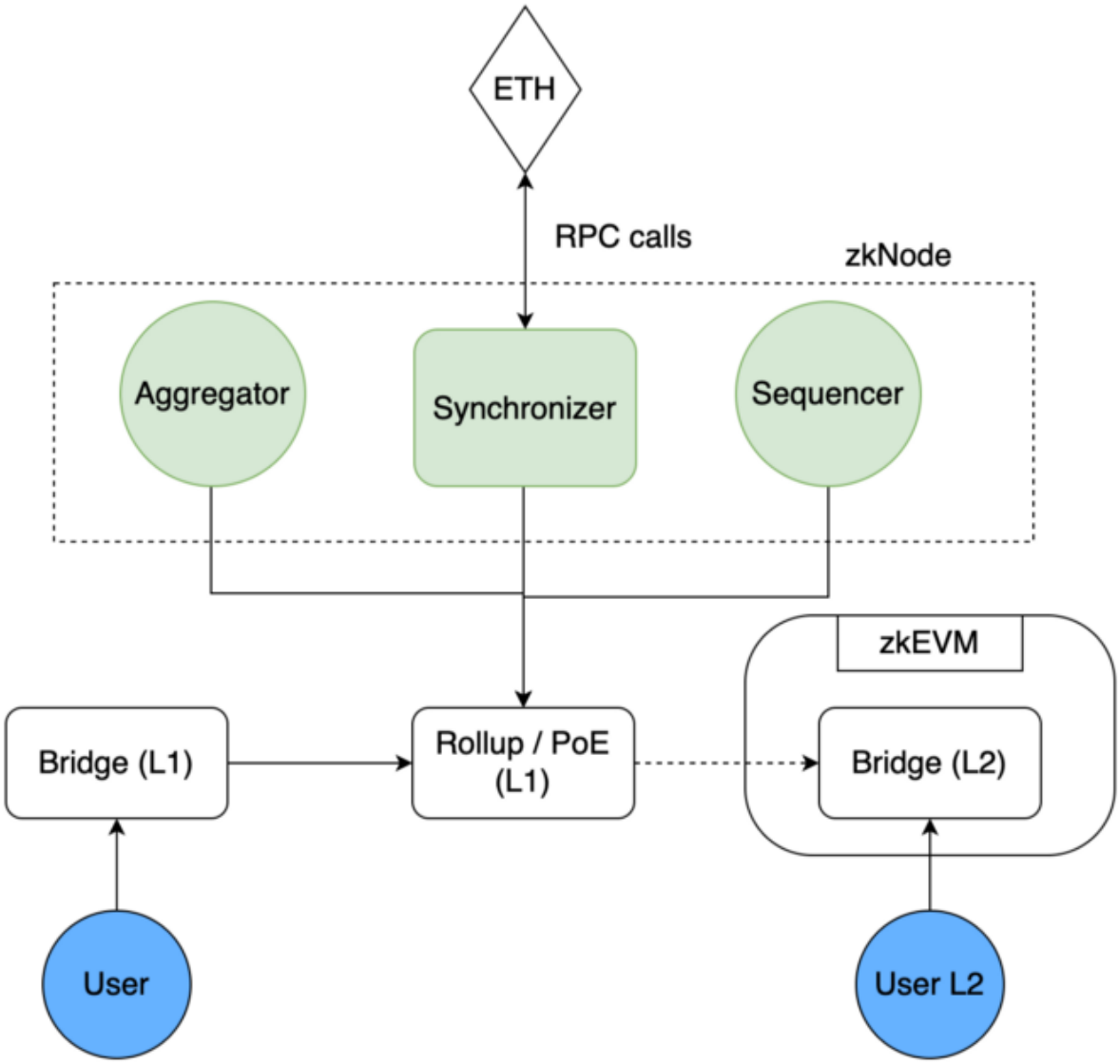
Polygon zk-EVM rollup is a breakthrough in zkRollups as it is the first zkRollup that offers full EVM compatibility, i.e. full compatibility at the EVM opcode level, not just at the Solidity level.

This allows developers to port any Ethereum smart contract over to the ZK rollup chain without changing the contract code.



Source: Polygon

zero-knowledge Ethereum Virtual Machine (zkEVM) generates zero-knowledge proofs to verify the correctness of batches of transactions submitted on a layer2. The zkProofs are then published on the ethereum Blockchain. Thus the security of layer1 Ethereum is obtained along with improved scalability.



(Architecture of Polygon zkEVM | Source: Polygon)

In every rollup, sequencers are responsible for managing the network. The sequencer processes transactions, produces rollup blocks and submits rollup transactions to the L1 chain. (Ethereum). Most of the sequencers for Optimistic Rollup and zk Rollup are centralized. So the sequencers are in a position to determine the transaction order.

zkEVM consists of sequencers, aggregators, and (POE) proof of efficiency consensus algorithm for implementing decentralization .

proof of efficiency consensus algorithm

The sequencers collect transactions in batches and proposes it to the network. The transaction batch created by sequencer is then submitted to the POE smart contract.The aggregator(prover) processes the transactions published by the sequencer and builds the validity proofs, which are then submitted to the ethereum network.

Proving and verifying transactions in **Polygon zkEVM** are handled by a zero-knowledge prover component in the aggregator called the **zkProver**. The **zkProver** performs complex mathematical computations and generates a proof which is sent to the POE smart contract to verify that the **validity Proof** from the **Prover** is correct. The PoE smart contract will accept as valid the first validity proof that updates to a new valid state and includes one or more of the proposed batches.

The L1-L2 in zkEVM

The L1-L2 in zkEVM is a decentralized bridge for secure deposits and withdrawal of assets. It is a combination of two smart contracts, one deployed on one chain and the second on the other.**Bridge L1 Contract** is on the Ethereum mainnet and manages asset transfers between rollups and **Bridge L2 Contract** is on a particular rollup and it is responsible for asset transfers between mainnet and the rollup

A synchroniser is required since batch submission and generation of validity proof is done separately on the zkEVM. The **Synchronizer** is responsible for getting all the data from Smart Contracts, which includes the data posted by the **sequencers** (transactions) and the data published by the **aggregators** (validity proofs). All this data is stored in a vast database and served to third parties through a **JSON-RPC** service that enables integration of the zkEVM with existing tools, such as Metamask, Etherscan, and Infura..

Summary of polygon zkEVM

zkEVM is a significant step towards decentralization of rollups as transaction proposal, and validation is separated using sequencer and aggregator. The EVM-compliant zk Rollup is expected to bring improvements in Ethereum ecosystem in aspects such as transaction throughput, Scalability and transaction fees. They also derive security from the Ethereum mainnet using zero knowledge proofs.

9. Conclusion

zkRollups presently on Mainnet, such as zksync 1.0, Aztec, Polygon Hermez, are explicitly used for payments. Universal rollups like Starknet, which support the deployment of various smart contracts, require the developers to write code in their own domain specific language called Cairo.

The Polygon zkEVM is expected to lead the race of zkRollups due to various features such as universality, EVM equivalence etc which will allow seamless processing of smart contracts.

The Polygon ecosystem will be the crucial player in scaling Ethereum as it also has various products like **Polygon Zero, Polygon Miden, Polygon Avail** which facilitate further adoption of modular blockchain solutions.