zkEVM

polygon

Thiago Lemos

Hi, I am

Thiago Lemos

Software Engineer

→ 17 years working w/ software development

→ Working with blockchain since 2021

→ zkEVM Node team member since the begining

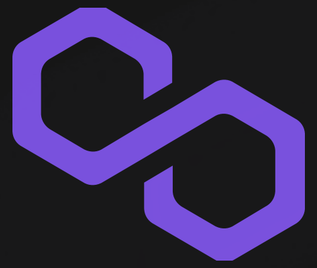


/@tclemos

Agenda

- Polygon Technology
- Problem
- Rollup and Zero Knowledge
- Protocol: Proof of Efficiency
- Strong points
- Use Cases
- Expectations

Who we are



Polygon Technology

Bringing the world to Ethereum

Polygon believes in Web3 for all. Polygon is a decentralized Ethereum scaling platform that enables developers to build scalable user-friendly dApps with low transaction fees without ever sacrificing on security.

Who we are

polygon

2017
Matic founded

2020
Mainnet Launch
PoS Chain

37K+
No. of dapps

135M+
Unique users

3M+
Daily transactions

2B+
Transactions since inception

Solutions

- Polygon PoS
- Polygon zkEVM
- Poligon Avail
- Polygon ID
- Polygon Nightfall
- Polygon Miden
- Polygon Zero

Ethereum Scalability

As the number of people using Ethereum has grown, the blockchain has reached certain capacity limitations. The main goal of scalability is to increase transaction speed (faster finality), and transaction throughput (high transactions per second), without sacrificing decentralization or security.

Problem

Ethereum

± 13
seconds per block

± 180
Txs per block

13~60
seconds to verify
a tx

Solution

Ethereum transparent scalability with L2 zk-Rollup

Polygon zkEVM is the first open-source zk-Rollup providing complete EVM opcode equivalence for a frictionless user experience and the security of Ethereum.

Solution

zk-Rollup

Rollup

Process transactions off-chain(L2) and store the state on chain(L1).

Zero Knowledge Proof

Prove that a statement is true without having to reveal any additional information apart from the fact that the statement is indeed true

zk-Rollup

Process transactions off-chain and prove they are valid sending a zk-proof proving they are valid.

Solution

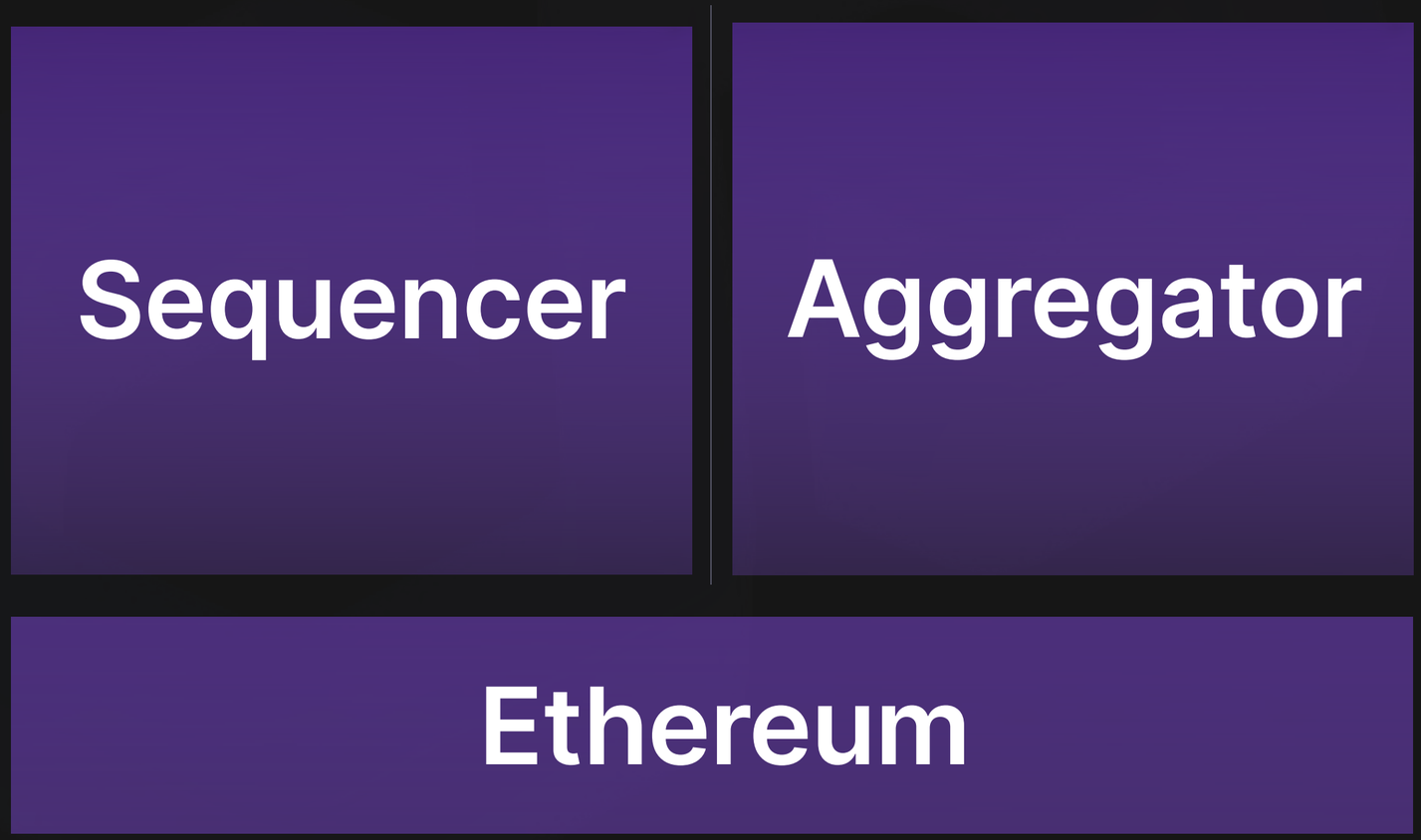
Proof of Efficiency

A new consensus mechanism for zk-rollups

Solution

Proof of Efficiency

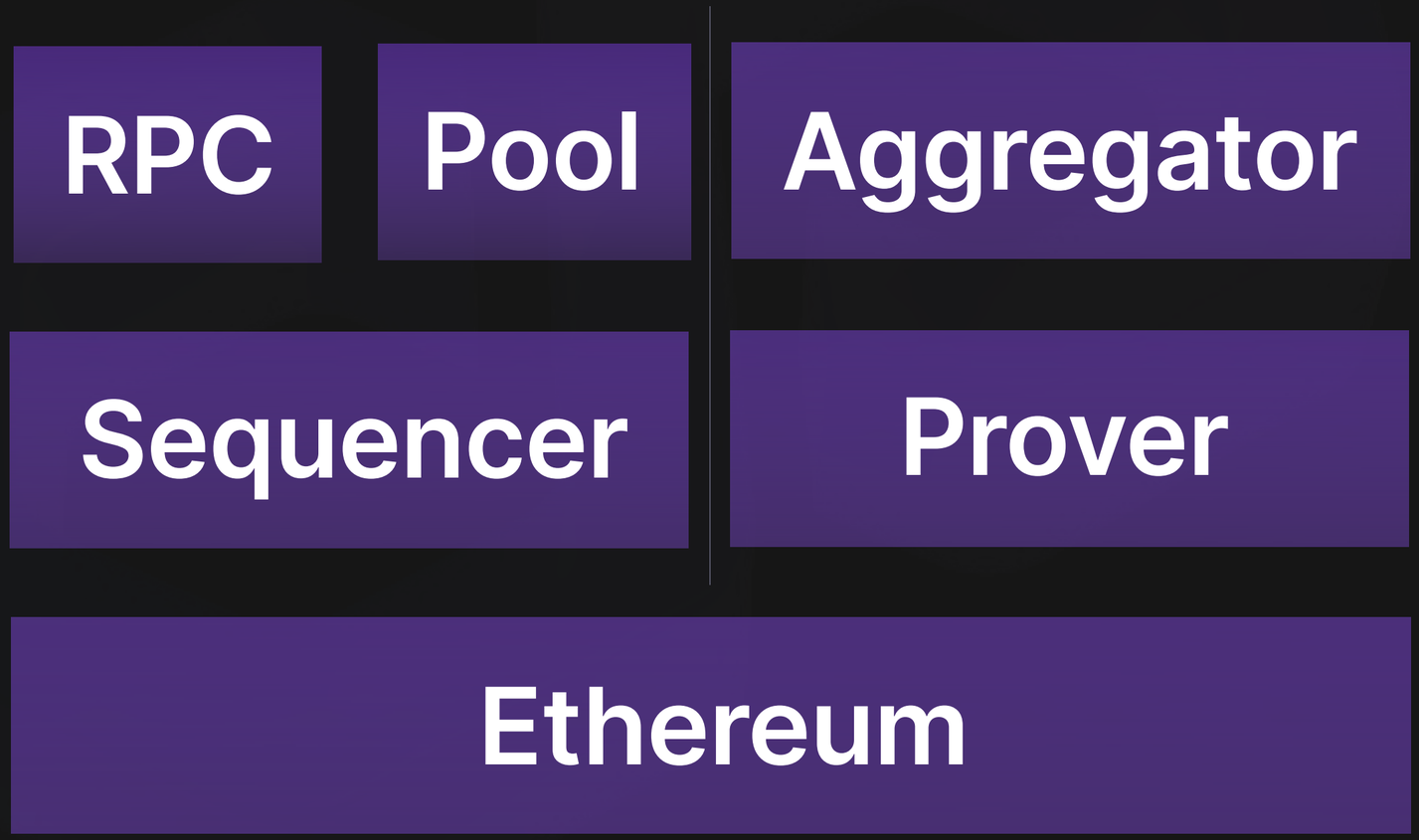
A new consensus mechanism for zk-rollups



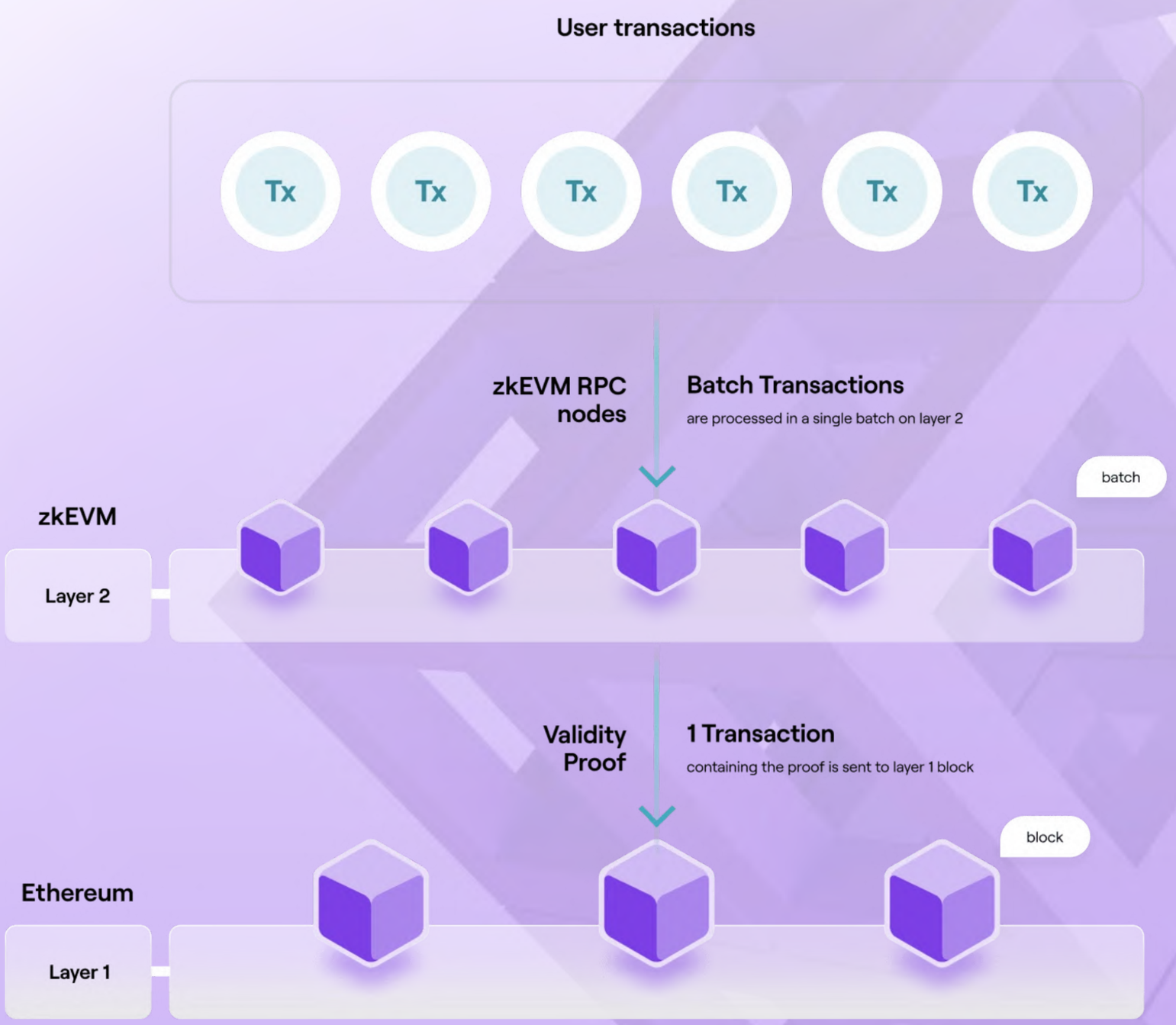
Solution

Proof of Efficiency

A new consensus mechanism for zk-rollups



Solution


User transactions
Tx
Tx
Tx
Tx
Tx
Tx
zkEVM RPC nodes
Batch Transactions
are processed in a single batch on layer 2
batch
zkEVM
Layer 2
Validity Proof
1 Transaction
containing the proof is sent to layer 1 block
block
Ethereum
Layer 1

Solution

Scaling without user friction

- Developers can run their existing Ethereum smart contracts
- Permissionless access and use of the network
- EVM equivalence means tooling compatibility
- Fast network finality with frequent validity proofs
- Fees reduction of 90% with on-chain data

Solution

No Compromises

- All EVM opcodes will be supported
- Ethereum security inherited in L2
- Censorship Resistance is enforced
- Decentralised by protocol design

Solution

Main Use Cases

- Defi Apps
- NFT and Gamefi
- Enterprise apps
- Payments

- Low fee
- Fast finality
- High security
- High throughput
- Censorship resistance

Solution

Ethereum Tests

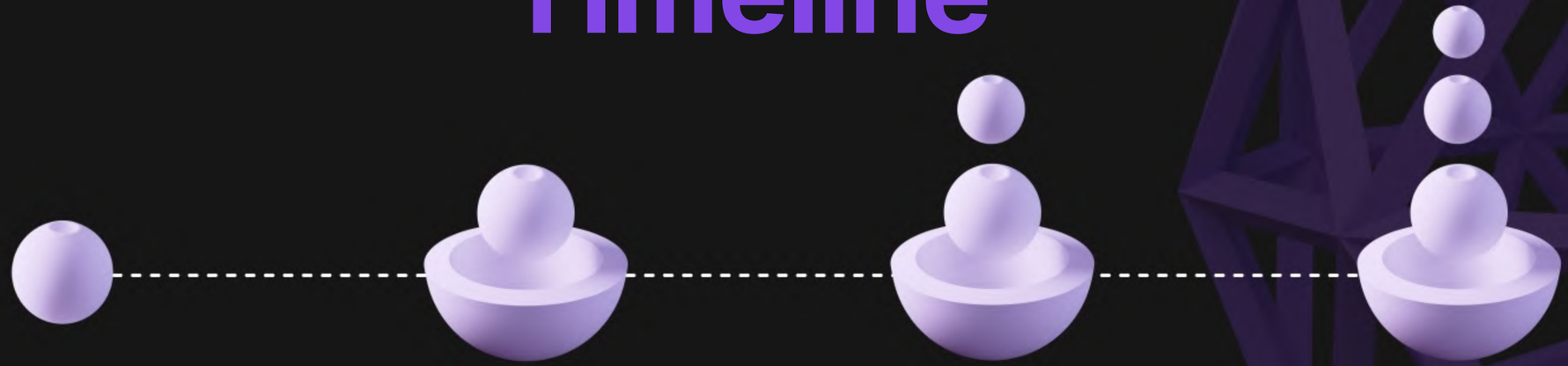
8336
Pass

72%
Coverage

* Coverage at July/2022: 28%

Solution

Timeline



Q1 2022

Research & Discovery

Q2 2022

Development

Q3 2022

Testnet

Early 2023

Mainnet

Solution

Open Source

/zkevm-doc

/zkevm-contracts

/zkevm-node

/zkevm-bridge-ui

/zkevm-prover

/zkevm-bridge-service

We are hiring

Go

Javascript

Solidity

C++

SCAN ME

Thank You

polygon

https://github.com/tclemos/zkevm-ethsp-2022