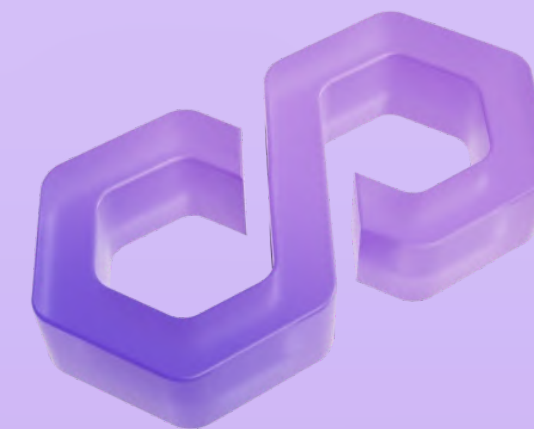
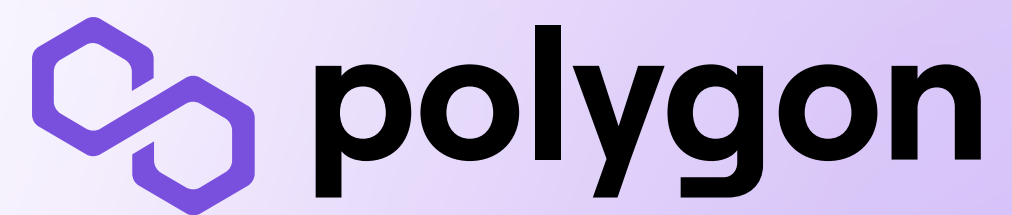


# zkEVM



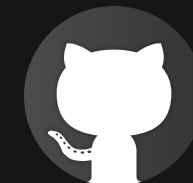
**Thiago Lemos**

Hi, I am

# Thiago Lemos

Software Engineer

- 17 years of software development experience
- Working with blockchain since 2021
- Member of zkEVM Node team since the beginning



# Agenda

● Polygon Tehcnology

● Problem

● Rollup and Zero Knowledge

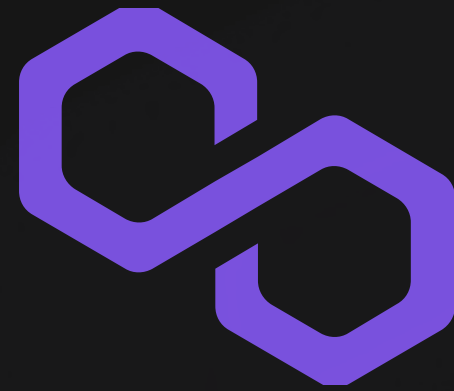
● Protocol: Proof of Efficiency

● Unique Values

● Use Cases

● Expectations

Who we are

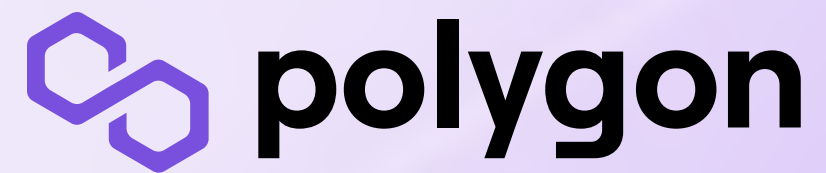


# Polygon Technology

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



**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



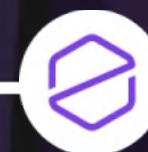
Polygon ID



Polygon Nightfall



Polygon Miden



Polygon Zero



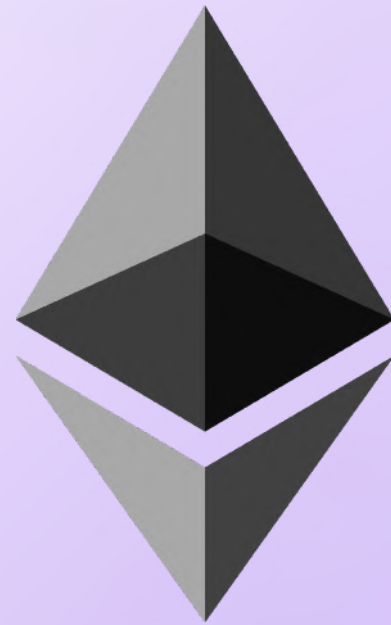
## Problem



# 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

$\pm 13$

seconds per block

$\pm 180$

Txs per block

$13 \sim 60$

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.

# 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

Sequencer

Aggregator

Ethereum

# Proof of Efficiency

A new consensus mechanism for zk-rollups

RPC

Pool

Aggregator

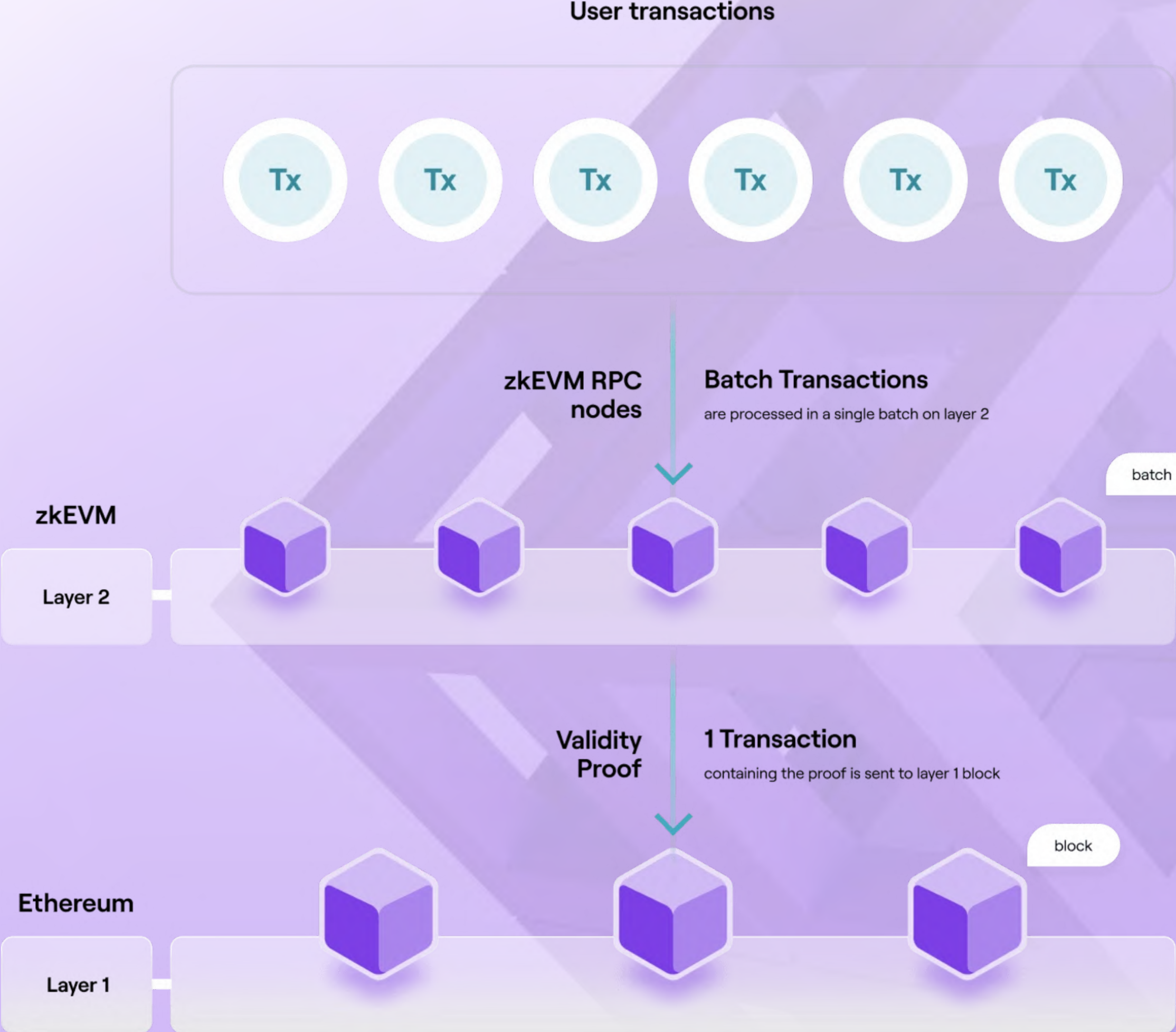
Sequencer

Prover

Ethereum



# Solution



# Scaling without user friction

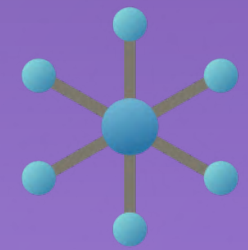
- ✓ **Developers can run their existing Ethereum smart contracts**
- ✓ **Permissionless access and use of the network**
- ✓ **EVM equivalence means tooling compatibility**
- ✓ **Fast network finality with frequent validity proofs**
- ✓ **Fees reduction of 90% with on-chain data**

# No Compromises

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



# Main Use Cases



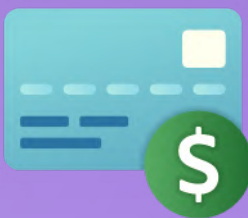
**Defi Apps**



**NFT and Gamefi**



**Enterprise apps**



**Payments**

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

# Ethereum Tests



8336

Pass



72%

Coverage

\* Coverage at July/2022: 28%



# Timeline



Q1 2022

Research  
&  
Discovery



Q2 2022

Development



Q3 2022

Testnet



Early 2023

Mainnet

# Open Source

 /zkevm-doc

 /zkevm-contracts

 /zkevm-node

 /zkevm-bridge-ui

 /zkevm-prover

 /zkevm-bridge-service

# We are hiring



Go



Solidity



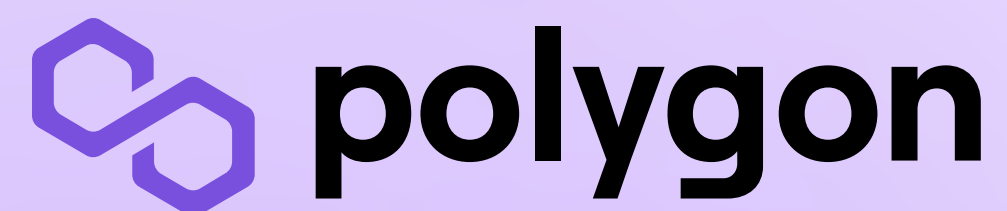
Javascript



C++



# Thank You



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