ZK Labs

A rollup that allows for scaling Tron without sacrificing security or compatibility.

MEET Zk Labs

Zk Labs is a L2 powered by zero knowledge technology.

zkEVM refers to an EVM equivalent and zk friendly virtual machine.

Zk Labs's execution layer uses MotionEVM, our ZK EVM-compatible runtime. This allows us to port existing EVM infrastructure while adding new features like parallel processing to the Tron network.

WHAT DOES IT DO?

☑ Eliminates the need for a native consensus protocol with ZK-proofs

☑ Sustain a throughput far higher than any L1

ZERO KNOWLEDGE ROLLUPS

- A zkRollup is a native layer 2 scaling solution which uses the blockchain for data avalability instead of computation, a smart contract holds all funds.
- For every batch of transactions, a zkSNARK cryptographic proof will be generated off-chain.
- This zkSNARK proves the validity of every transaction in a batch which means it is not necessary to rely on the blockchain to verify each signature transaction.

- The significance of this is that it allows verification to be carried out constantly regardless of the number of transactions. This ability to verify proofs efficiently and constantly is at the heart of all zkRollups.

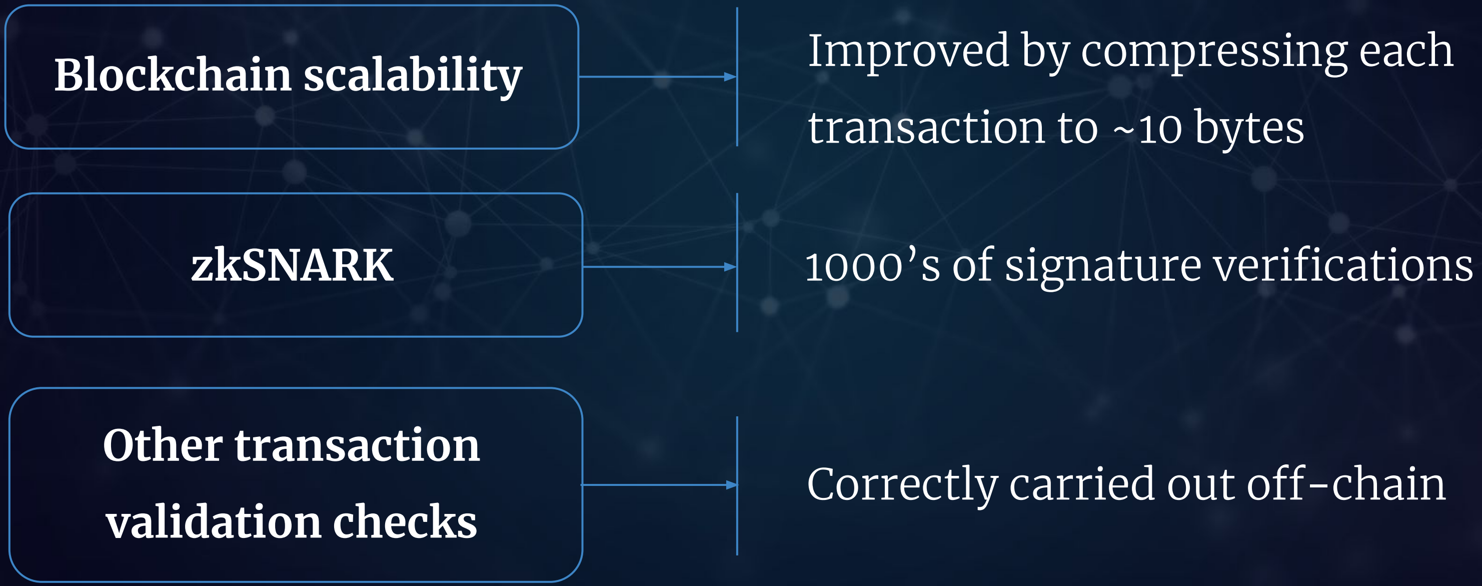
- All transaction data is published relative cheaper on-chain, without signatures — under calldata. Since the data is published on-chain, no data availability problems have plagued other L2 solutions such as Plasma.

INITIAL DEPLOYMENT IN ZK Labs

For improving the usability of a variety of dApps on ZK Labs

- ☑ Decentralized central limit order books (CLOBs)
- ☑ Games that utilize high TPS
- ☑ dApps that rely on CLOB infrastructure
- ☑ Trading real-world assets (RWAs) with sizeable oracle data
- ☑ Notifications and messaging
- ☑ Private Blockchain Execution
- ☑ Private Cloud and Privacy centric applications

2000 TPS: IT’S POSSIBLE!

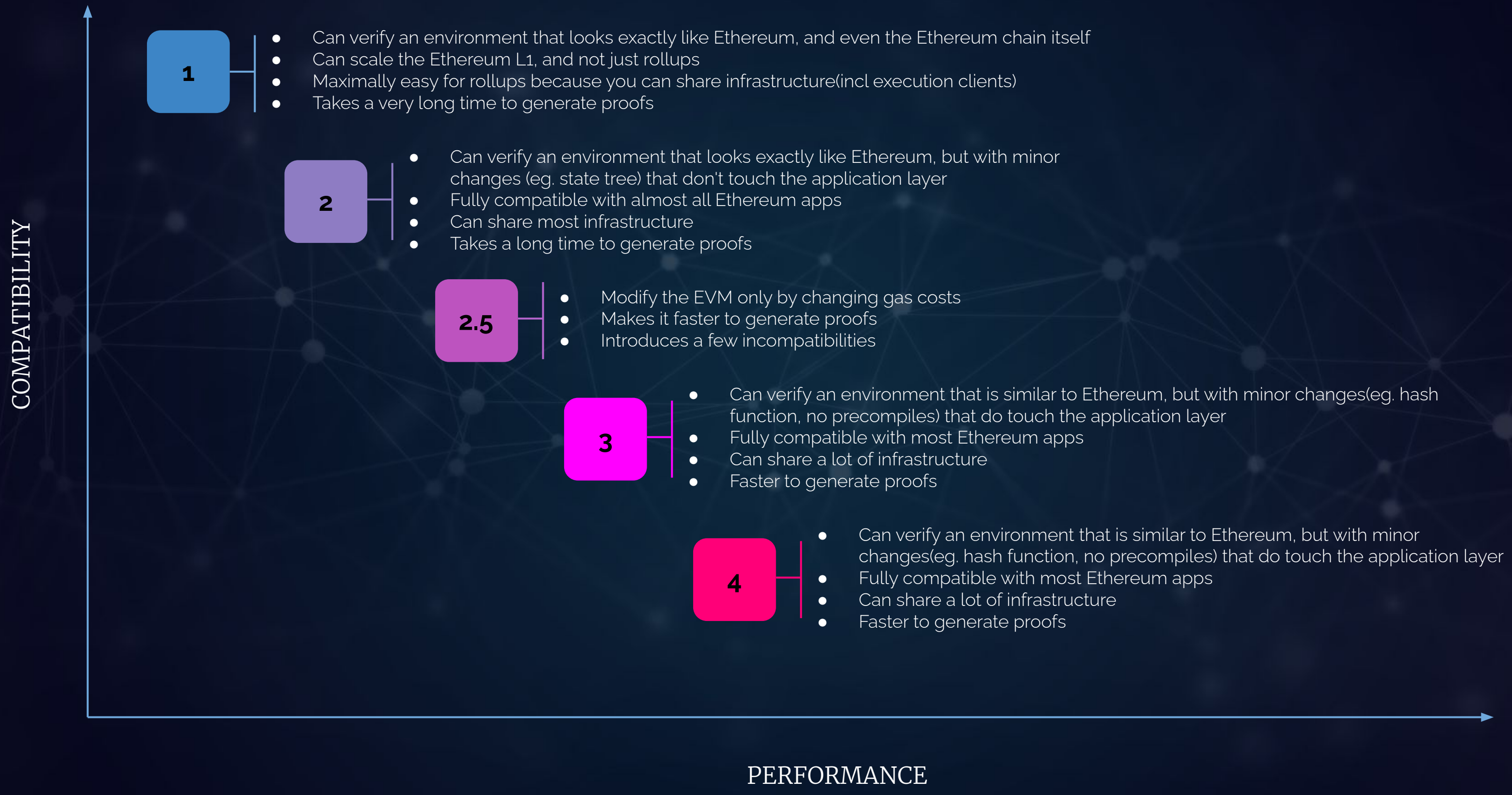


Blockchain scalability → Improved by compressing each transaction to ~10 bytes

zkSNARK → 1000’s of signature verifications

Other transaction validation checks → Correctly carried out off-chain

OVERVIEW



1

- Can verify an environment that looks exactly like Ethereum, and even the Ethereum chain itself
- Can scale the Ethereum L1, and not just rollups
- Maximally easy for rollups because you can share infrastructure(incl execution clients)
- Takes a very long time to generate proofs

2

- Can verify an environment that looks exactly like Ethereum, but with minor changes (eg. state tree) that don't touch the application layer
- Fully compatible with almost all Ethereum apps
- Can share most infrastructure
- Takes a long time to generate proofs

2.5

- Modify the EVM only by changing gas costs
- Makes it faster to generate proofs
- Introduces a few incompatibilities

3

- Can verify an environment that is similar to Ethereum, but with minor changes(eg. hash function, no precompiles) that do touch the application layer
- Fully compatible with most Ethereum apps
- Can share a lot of infrastructure
- Faster to generate proofs

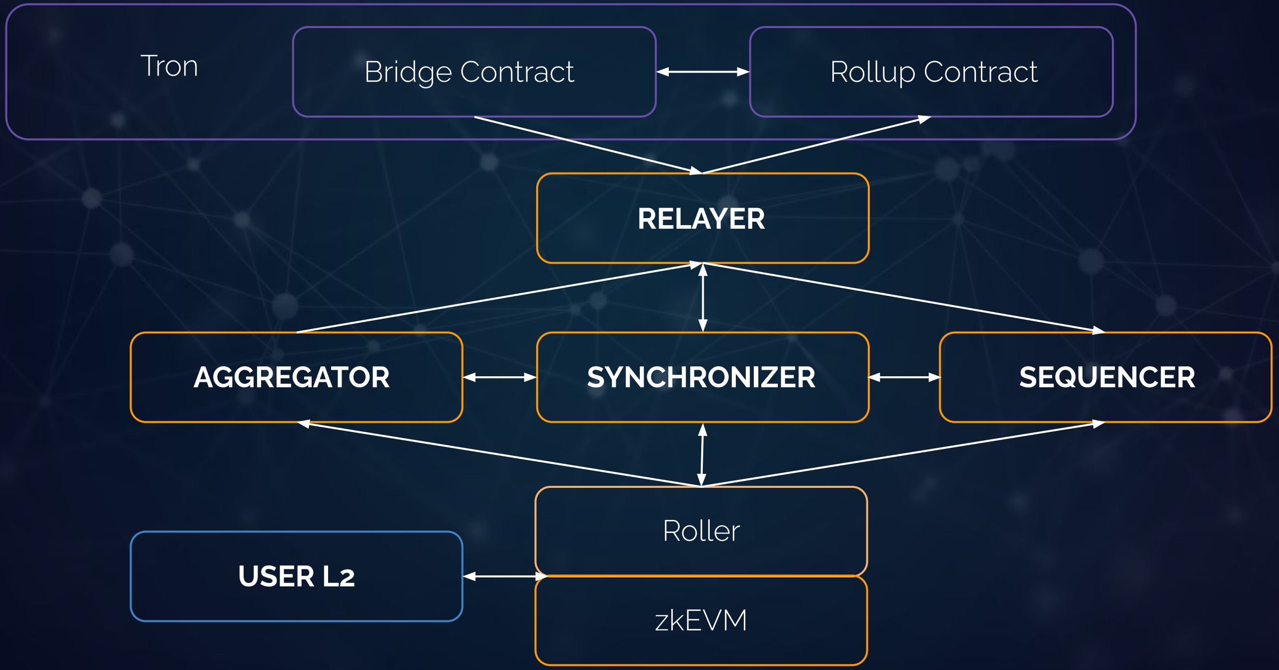
4

- Can verify an environment that is similar to Ethereum, but with minor changes(eg. hash function, no precompiles) that do touch the application layer
- Fully compatible with most Ethereum apps
- Can share a lot of infrastructure
- Faster to generate proofs

BASIC COMPONENTS

- ☑ Proof of Efficiency (PoE) consensus mechanism.
- ☑ zkNode software, including a synchroniser, sequencer and aggregator.
- ☑ LX-to-LY bridge.
- ☑ zkProver.
- ☑ Active users of the zkEVM network who create transactions.

BASIC COMPONENTS



HYBRID MODE FOR ON-CHAIN DATA AVAILABILITY

zkProver is composed of the following four components:

- ☑ The Executor, which is the Main State Machine Executor
- ☑ The STARK Recursion Component
- ☑ The CIRCOM Library
- ☑ The zkSNARK Prover

TEAM

Yu Huang, CTO

PhD in Cryptography, Peking University.

Several academic papers related to cryptography published.

Years of experience in design and implementation of underlying cryptographic algorithms for multiple blockchain projects.

Tech-lead at multiple EVM-compatible anonymous public chains and currency mixing protocols.

Finch Luo, Core Developer

MSc in Math, The Hong Kong Polytechnic University.

Specializing in ZKP and public chain architecture.

Yie-Sean Teoh, Co-founder

BSc in Economics, The London School of Economics

Listing and BD department head at Poloniex

CFA qualified with several years of experience in Traditional Finance

Elias Juan, Development Engineer

PhD in Computer Science, National University of Singapore

Years of experience as core algorithmic engineer, responsible for t technical framework construction and R&D at multiple blockchain projects.

ZK LABS, incubated by Zebec

Zebec