Advancing OP Stack to ZK Rollup

Achieving Efficiency and Security with Zero Knowledge Proofs

TA (fakedev9999)

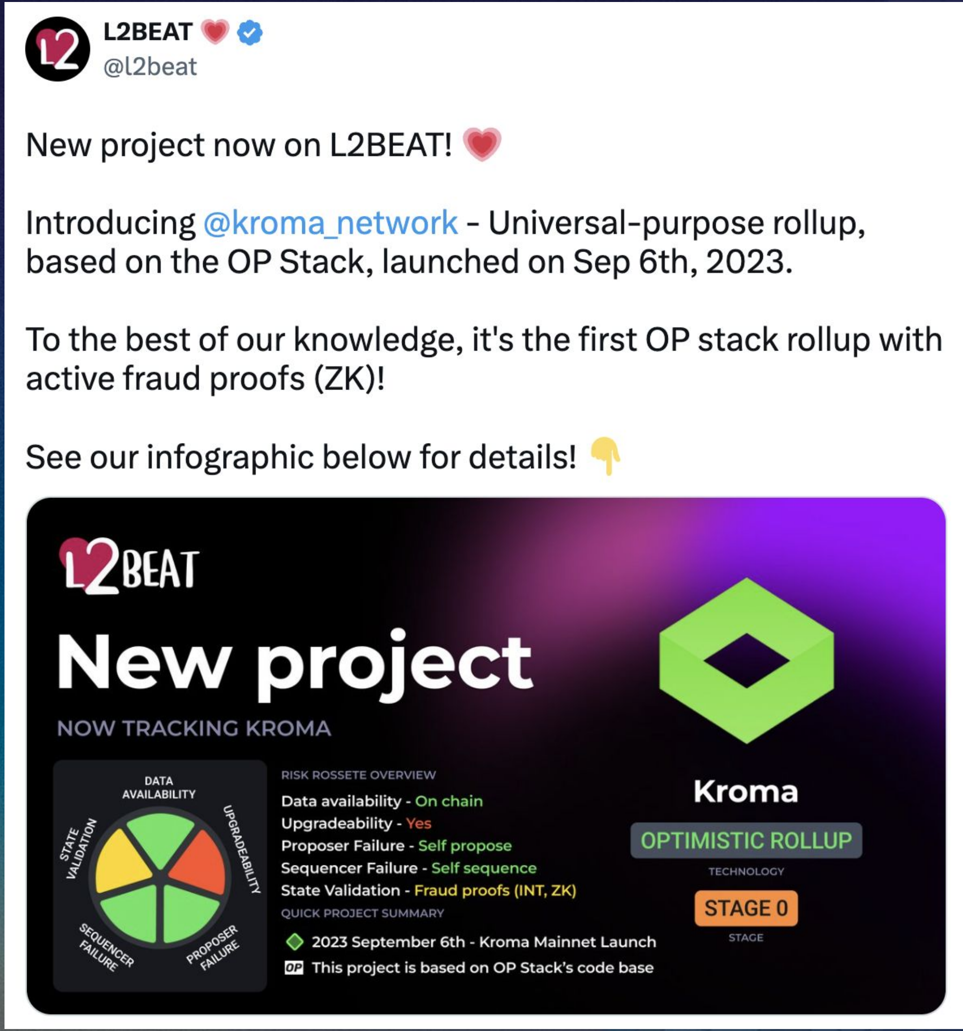
ZK Engineer, Kroma

Section 1

First, let’s celebrate our successes

First, let's celebrate our successes

- Solved problems in fault proofs
- Transitioning from circuits to zkVMs
- Pushing boundaries on proof generation speed



L2BEAT ❤️
@l2beat

New project now on L2BEAT! ❤️

Introducing @kroma_network - Universal-purpose rollup, based on the OP Stack, launched on Sep 6th, 2023.

To the best of our knowledge, it's the first OP stack rollup with active fraud proofs (ZK)!

See our infographic below for details! 👇

L2BEAT

New project

NOW TRACKING KROMA

RISK ROSSETE OVERVIEW

Data availability - On chain
Upgradeability - Yes
Proposer Failure - Self propose
Sequencer Failure - Self sequence
State Validation - Fraud proofs (INT, ZK)

QUICK PROJECT SUMMARY

2023 September 6th - Kroma Mainnet Launch
OP This project is based on OP Stack's code base

Kroma

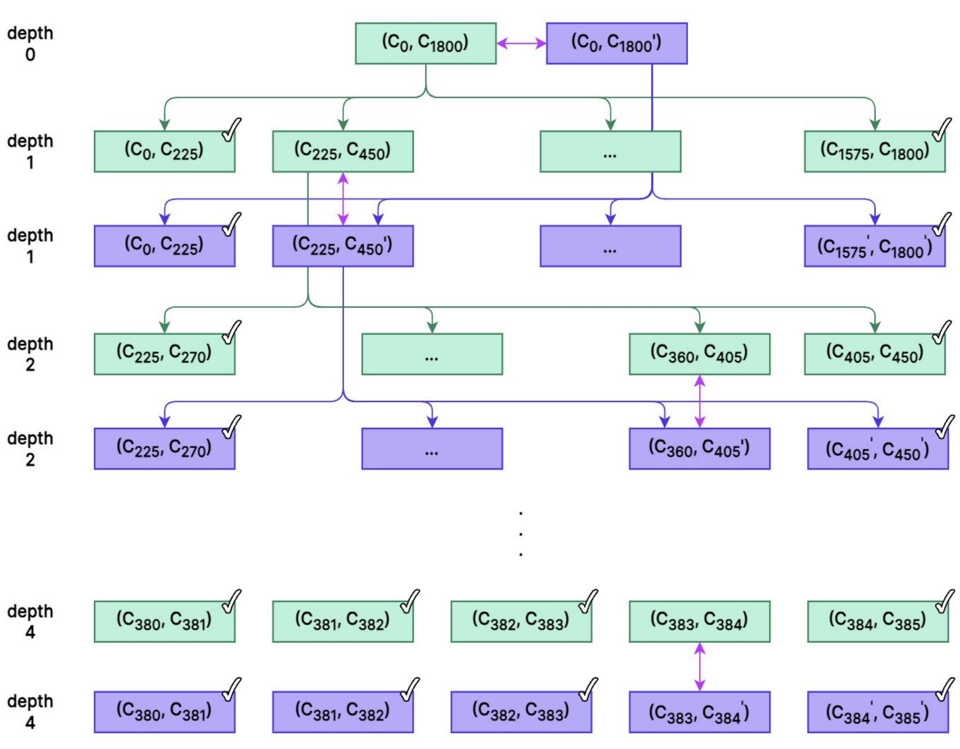
OPTIMISTIC ROLLUP
TECHNOLOGY

STAGE 0
STAGE

Why ZK Fault Proofs?

Costs reduced

- By number of interactions reduced
  - Lowers Operational Cost & Bond Requirement
  - Better decentralization & security



depth 0
(C_0, C_{1800}) (C_0, C_{1800}')

depth 1
(C_0, C_{225}) ✓ (C_{225}, C_{450}) ... (C_{1575}, C_{1800}) ✓

depth 1
(C_0, C_{225}) ✓ (C_{225}, C_{450}') ... (C_{1575}', C_{1800}') ✓

depth 2
(C_{225}, C_{270}) ✓ ... (C_{360}, C_{405}) (C_{405}, C_{450}) ✓

depth 2
(C_{225}, C_{270}) ✓ ... (C_{360}, C_{405}') (C_{405}', C_{450}') ✓

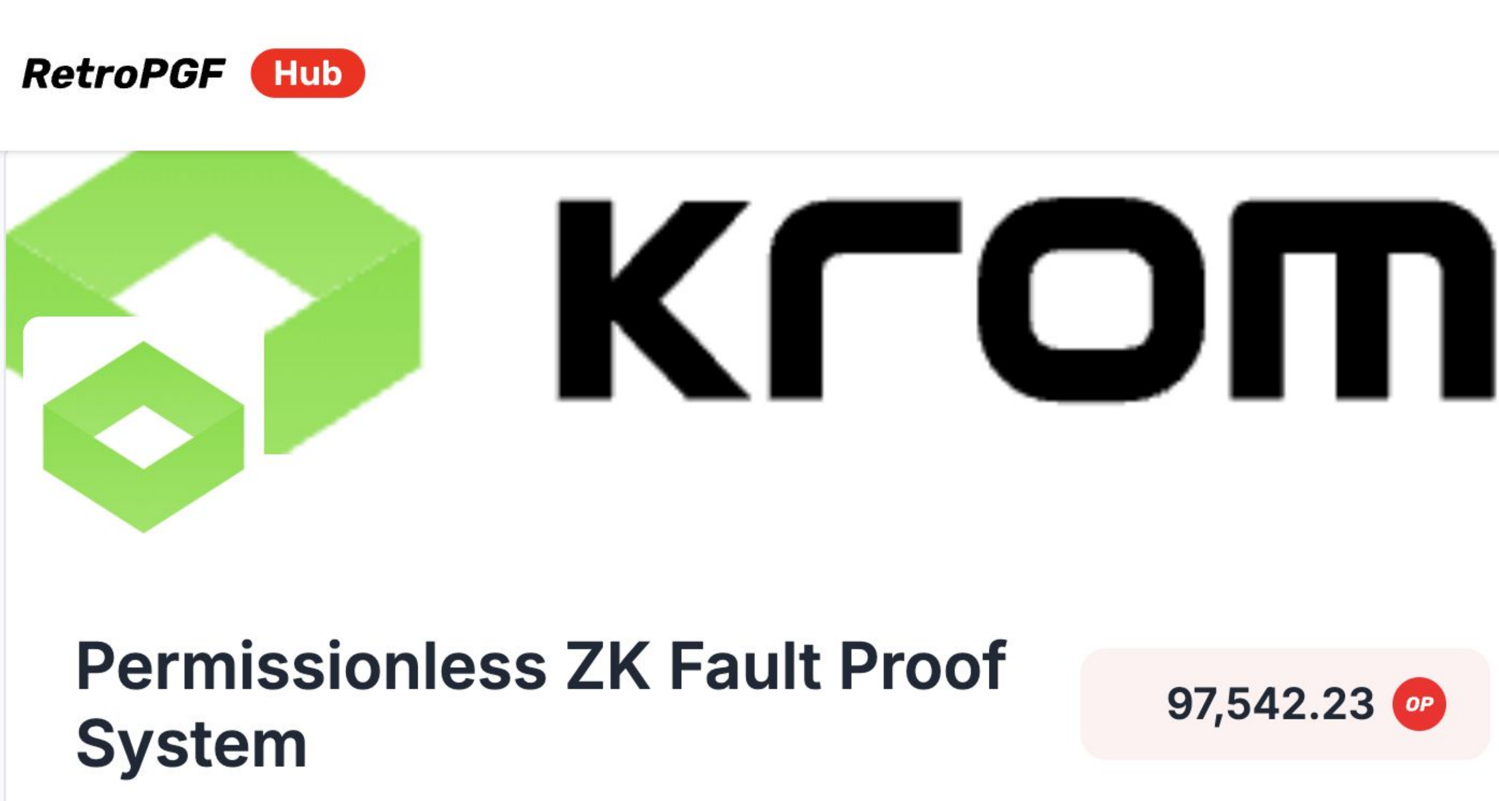
depth 4
(C_{380}, C_{381}) ✓ (C_{381}, C_{382}) ✓ (C_{382}, C_{383}) ✓ (C_{383}, C_{384}) ✓ (C_{384}, C_{385}) ✓

depth 4
(C_{380}, C_{381}) ✓ (C_{381}, C_{382}) ✓ (C_{382}, C_{383}) ✓ (C_{383}, C_{384}') (C_{384}', C_{385}') ✓

Bond amount required

Network	ZK Fault Proof?	Bond Requirement
Arbitrum	X	3600 ETH
Optimism	X	Max 700 ETH
Kroma	O	0.2 ETH

Retro PGF Round 5 Result



RetroPGF Hub

Permissionless ZK Fault Proof System

97,542.23 OP

Section 2

Challenges and Lessons Learned

Challenges and Lessons Learned

Circuit based approach is not sustainable

- 100,000 LOC, custom circuits to check integrity of EVM STF
- ***"Not going to be bug-free for a long long time"*** *- Vitalik in 2022*

Limitations of the Circuit-Based Approach

- Writing circuits is tough
- Supporting protocol upgrades in Ethereum and Optimism

Circuit Based vs. zkVM Based

Approach	Circuit Based	zkVM Based
Language	Plonkish	Rust
Auditability	No	Yes

zkVMs with Generality and Auditability

Section 3

From circuits to zkVMs

zkVMs provide general-purpose environment

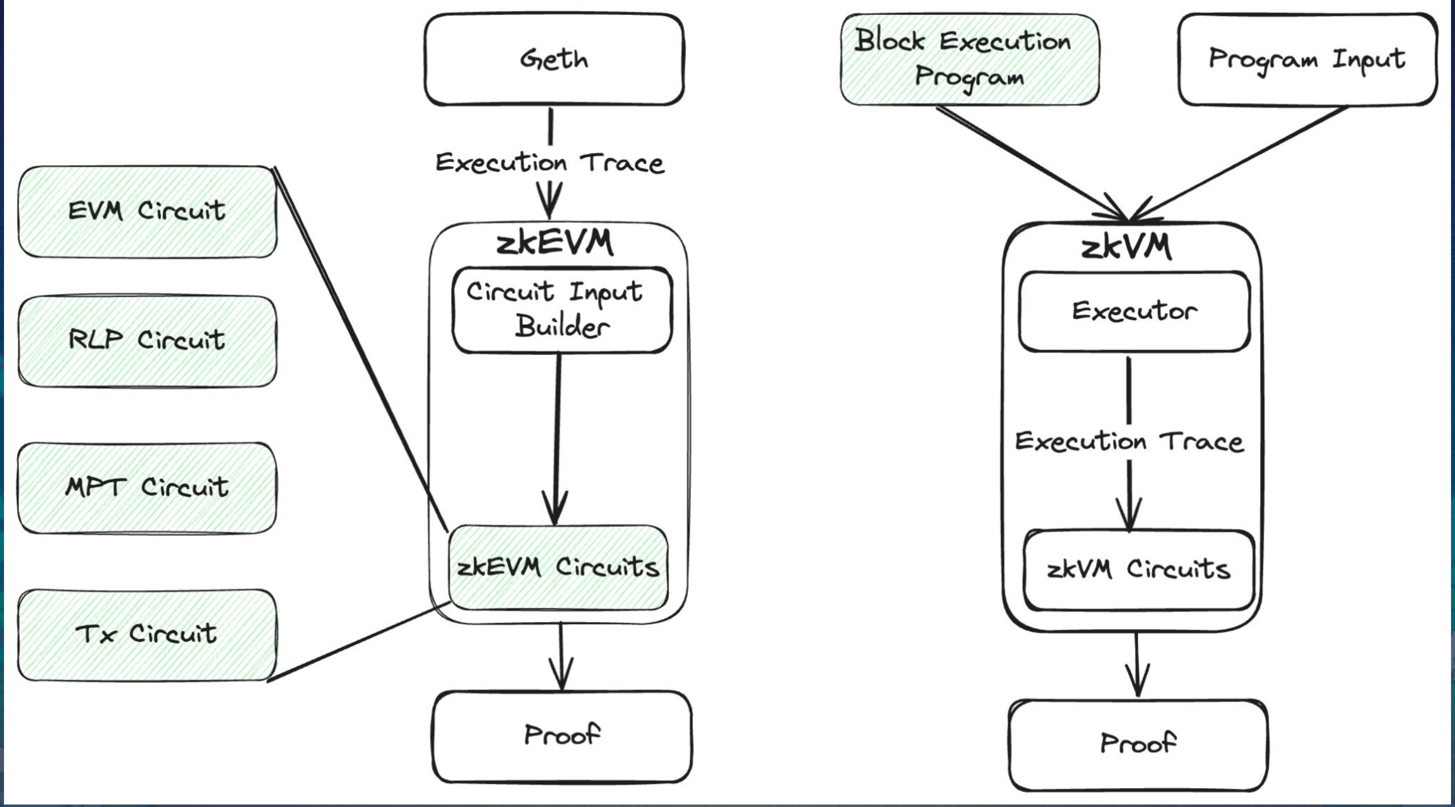
No more circuits, just Rust

Guarantees the integrity of computations

- Compiles into machine code
- Executes and generates execution trace
- Commits to the trace and generates proof

Circuit based approach vs. zkVM based approach

100K LOC



200 LOC

The Breakthrough: Sharding

Why not zkVMs at first?

Not sufficiently performant at that time

- Potential vulnerability to delay attacks

Sharding/Continuation

- Divides execution into “shards”
  - SP1: 2^{22} RISC-V cycles
- Enables parallel proof generation

Section 4

The Path Forward: Overcoming Barriers to ZK Rollups

Concerns about zkVM based approach

What if the zkVM Prover Network fails?

- Need multi machine orchestration implementation for decentralization
- How to make failure on-chain provable?

zkVM is not a Silver Bullet

Multi Prover Matters

Enhance security with not much overhead

- TEE Provers
- Another Circuit based zkEVM
- **Another zkVM based zkEVM**

Proofs are prone to errors

Challenges to ZK Rollup Feasibility

Current Cost Barriers

- $1M / year proving cost for 3 TPS

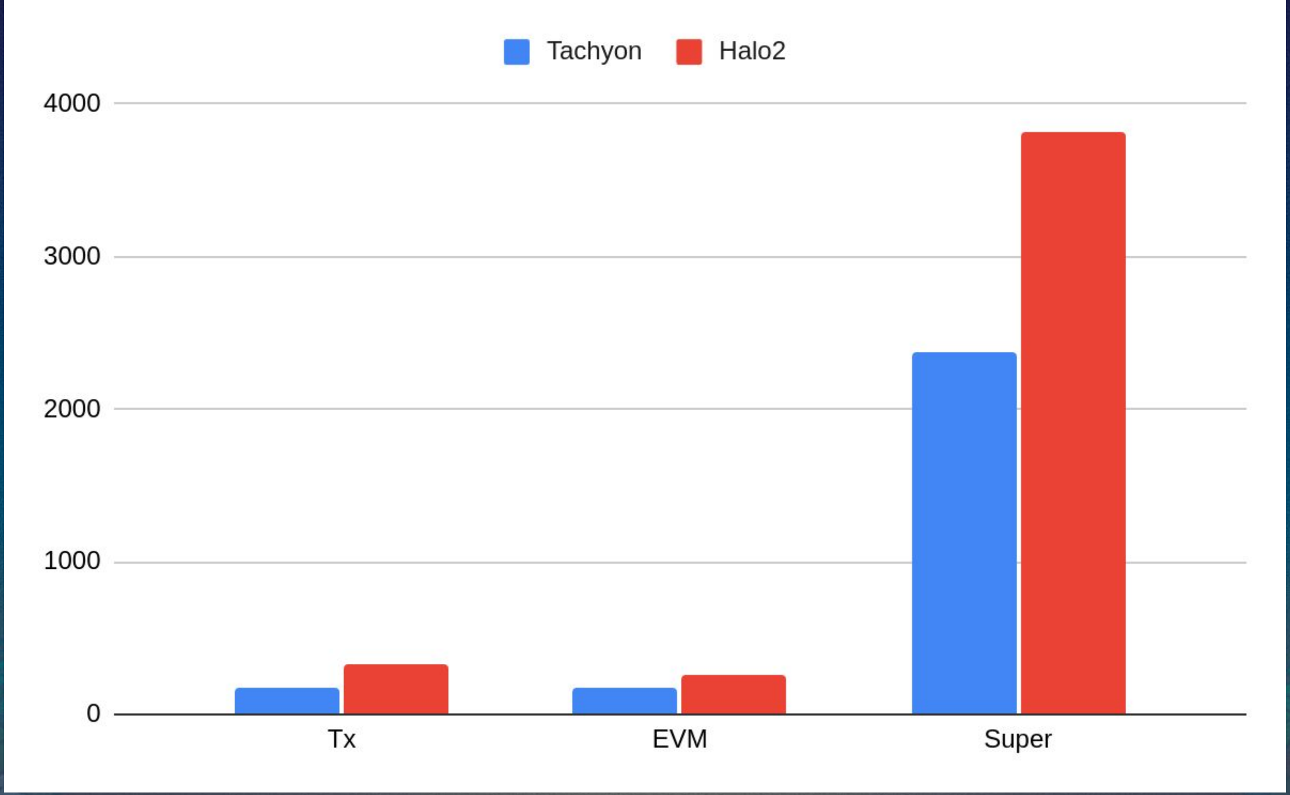
  + Settlement fees

  + Verification fees

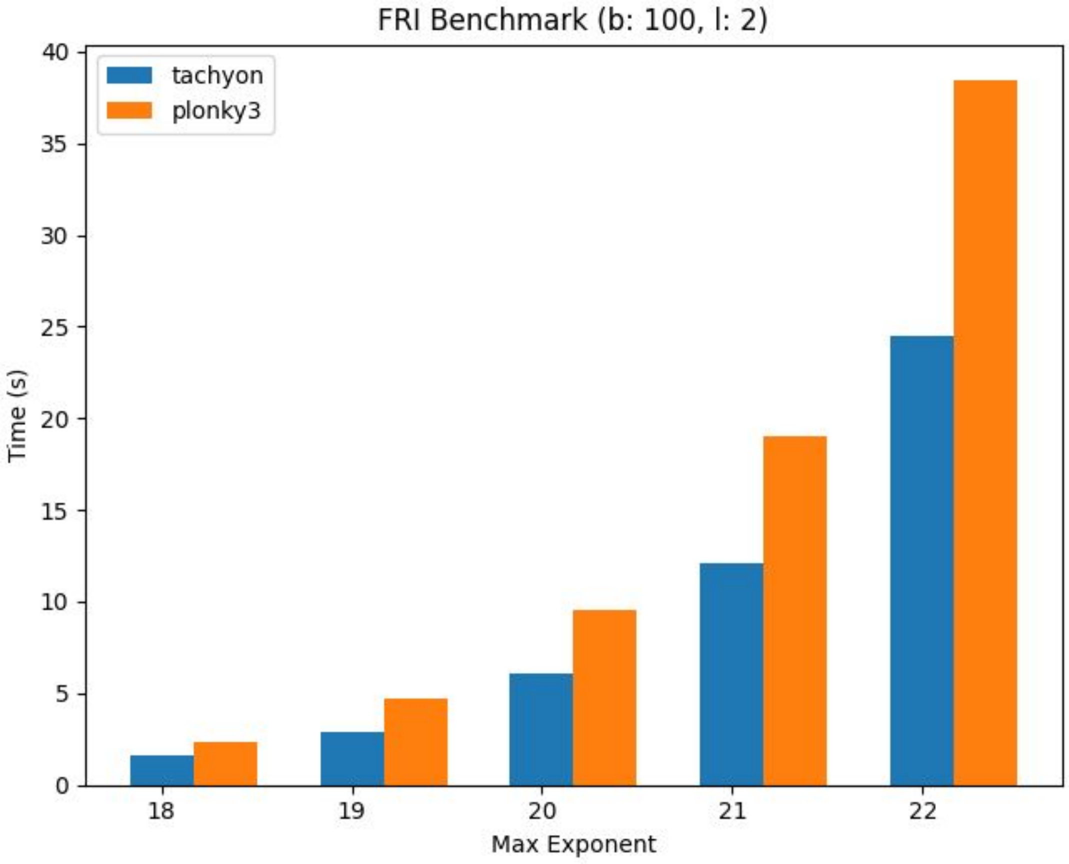
Future Directions

- Multi Prover System
- Prover Decentralization

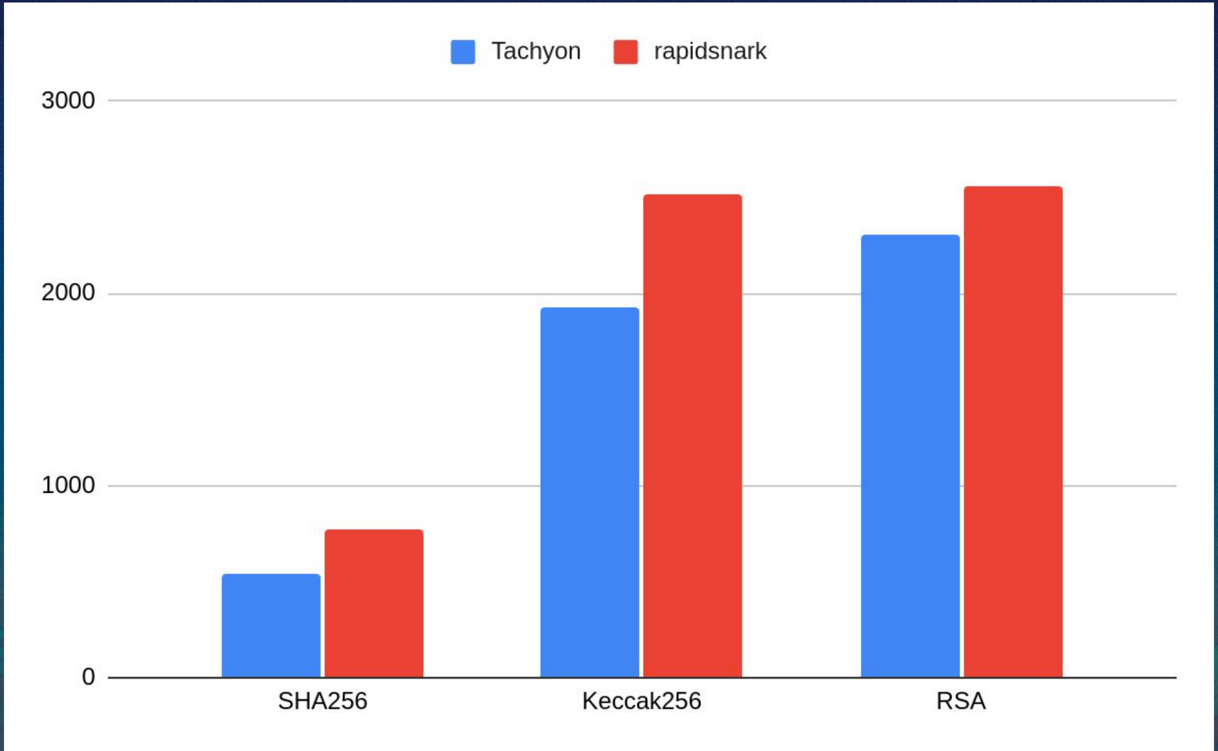
Pushing the boundaries of Proof Generation



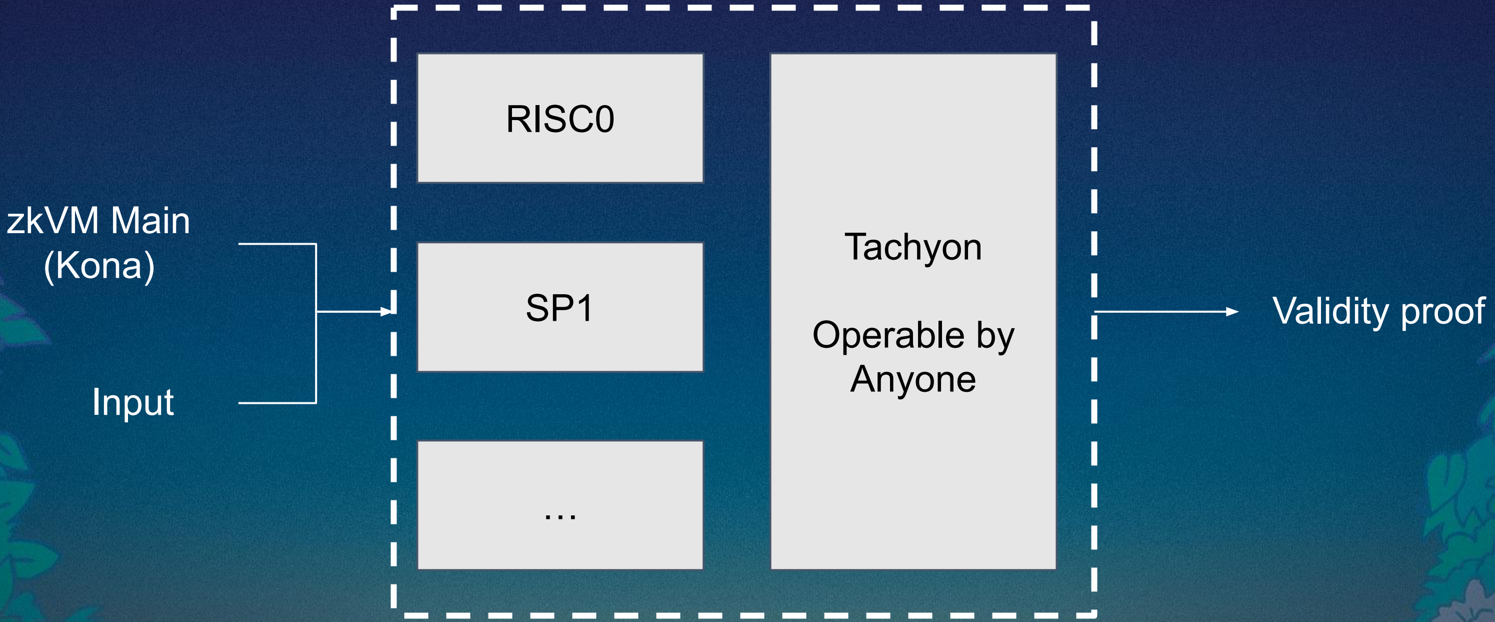
Pushing the boundaries of Proof Generation



Pushing the boundaries of Proof Generation



Multi zkVM Provers backed by Tachyon



Thank you!

TA (fakedev9999)

ZK Engineer, Kroma

ta@lightscale.io

@fakedev9999