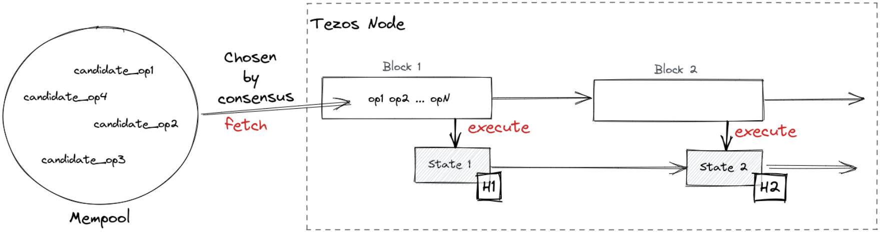
Scaling Tezos with Optimism

Yann Régis-Gianas

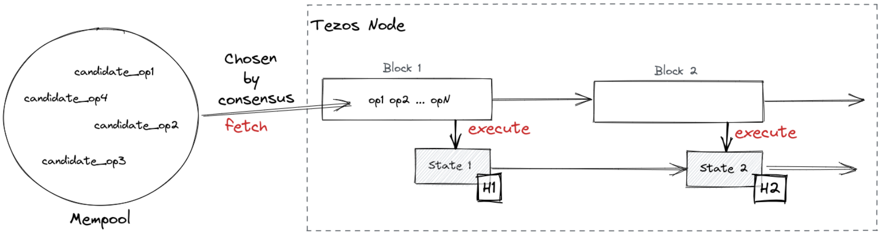
(Nomadic Labs) – yann.regis-gianas@nomadic-labs.com

2022-06-01

A blockchain is a super demanded computer



A blockchain is a super demanded computer



A real-time system

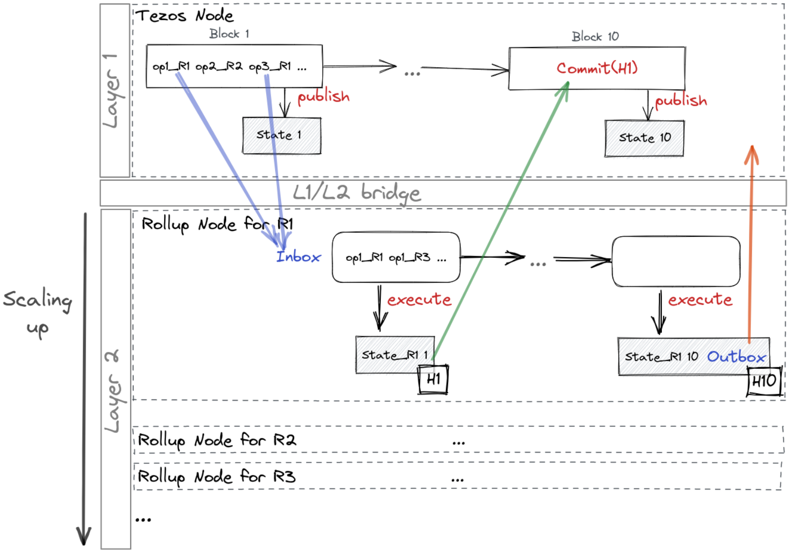
- 1 block every 30 seconds.
- Block validation should take less than 10 seconds.
- Limit block size and gas ($\simeq$ computational cost).
- Hard to go beyond 1000 operations per second.

What if we wanted this computer
to handle 1 million operations per second?

Make the CPU faster?

- By optimizing the **execute** step.
- We already had a 10x improvement with a fast interpreter.
- With compilation, we could get an extra 10x.
- Several orders of magnitude are still missing...

Let's increase the number of CPUs!

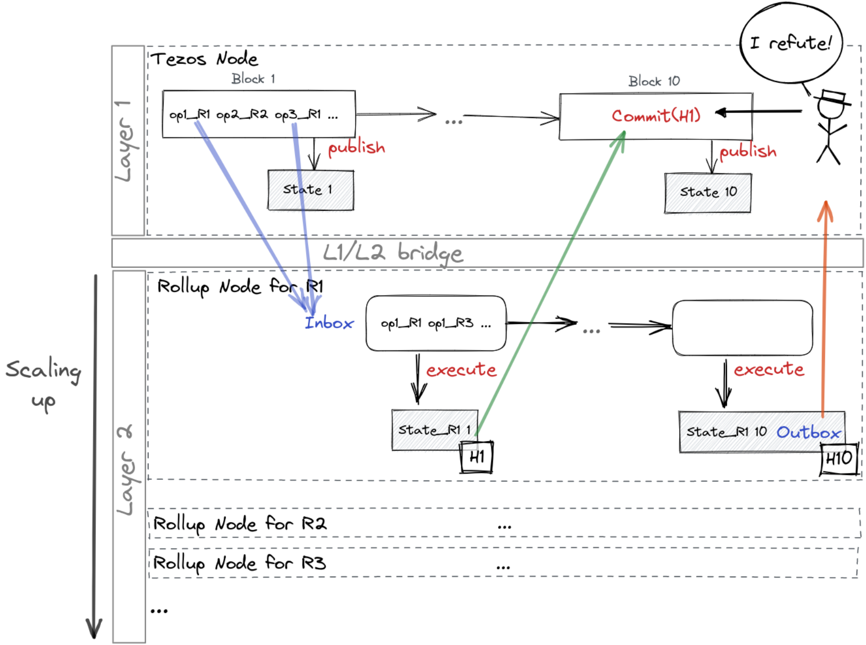


That’s scaling! but wait, is that really safe?

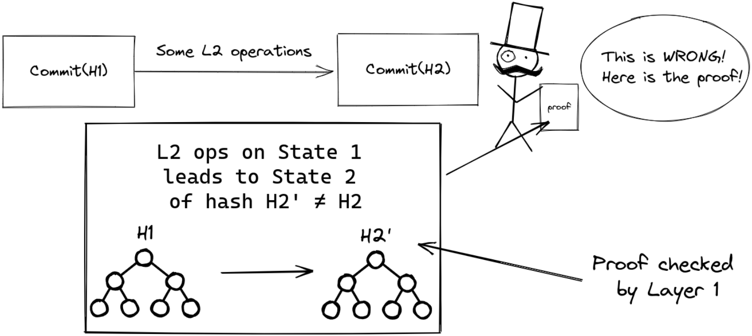
- This scheme can scale to infinity and beyond! [1]
- The layer 1 is **optimistic** regarding rollups execution.
- But, a dishonest rollup operator can forge and commit any hash!

[1] Well, no, we will come back to this.

Refutation at the rescue



What exactly is a refutation? Why should we fear them?



- A **Merkle tree** provides a compact partial representation of states.
- If a hash is proved wrong, its author is **economically punished**.

Good! But these refutation proofs are limited

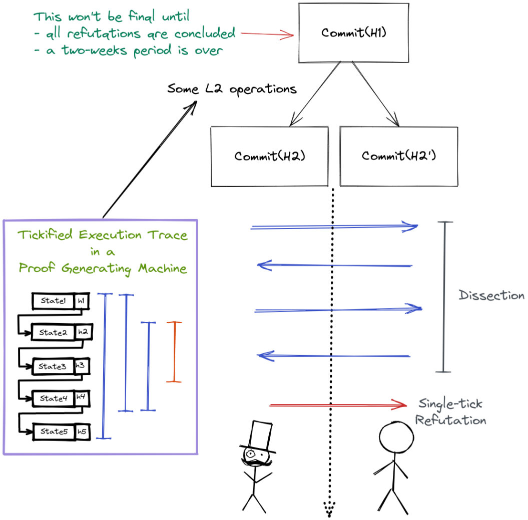
Transaction Optimistic Rollups (TORUs)

- TORUs are in protocol Jakarta2.
- 1000 transactions per second.

Limitations

- A Tezos operation is 32KB long.
- Even though Merkle proofs are compact, this limit is hit quickly.
- TORUs are only limited to transactions, no smart-contracts.

Interactive refutation through Proof Generating Machines (PVMs)



This won't be final until
- all refutations are concluded
- a two-weeks period is over

Commit(H1)

Some L2 operations

Commit(H2)

Commit(H2')

Tickified Execution Trace
in a
Proof Generating Machine

Dissection

Single-tick
Refutation

Smart-Contract Optimistic Rollups (SCORUs)

Unleashing the computational power of the blockchain

- A single-tick refutation proof is small enough.
- The execution trace can be very large (32^{10} is still fine).
- The system is generic with respect to the PVM.
- SCORUs are to be shipped in protocol K with a WASM PVM.
- Goal: demonstrate one million transactions per second by EOY.

Bandwidth is the bottleneck

- All operations are published by the Layer 1.
- Hence, we are limited by the size of the block ($\simeq$ 500KB).
- The Data Availability Layer (effort led by François Thiré) will tackle this.

Some open challenges

A challenge in Programming

Remarks

- Refutations are uncommon.
- Rollup nodes can run on powerful machines.

How to execute L2 operations as fast as possible
while being able to generate Merkle proofs
when a refutation occur?

A challenge in Mechanized Verification of Runtime System

Remarks

- The Layer 1 serves as the source of truth regarding PVM semantics.
- Rollup node implementations will run optimized runtime systems.

How to guarantee that an optimized runtime

- validates the PVM semantics?
- generates valid proofs?
- generates sufficiently small proofs?

A challenge in Game Theory

How to set the economic rules
so that the cost of an attack
is always greater than a given constant?

Thank you for your attention.
Questions?