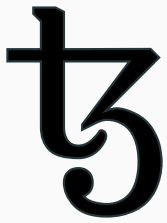


Formal Verification of the Tezos Blockchain Protocol

Zaynah Dargaye, Germán Andrés Delbianco, Kim Quyen Ly, Boubacar Demba Sall, François Thiré

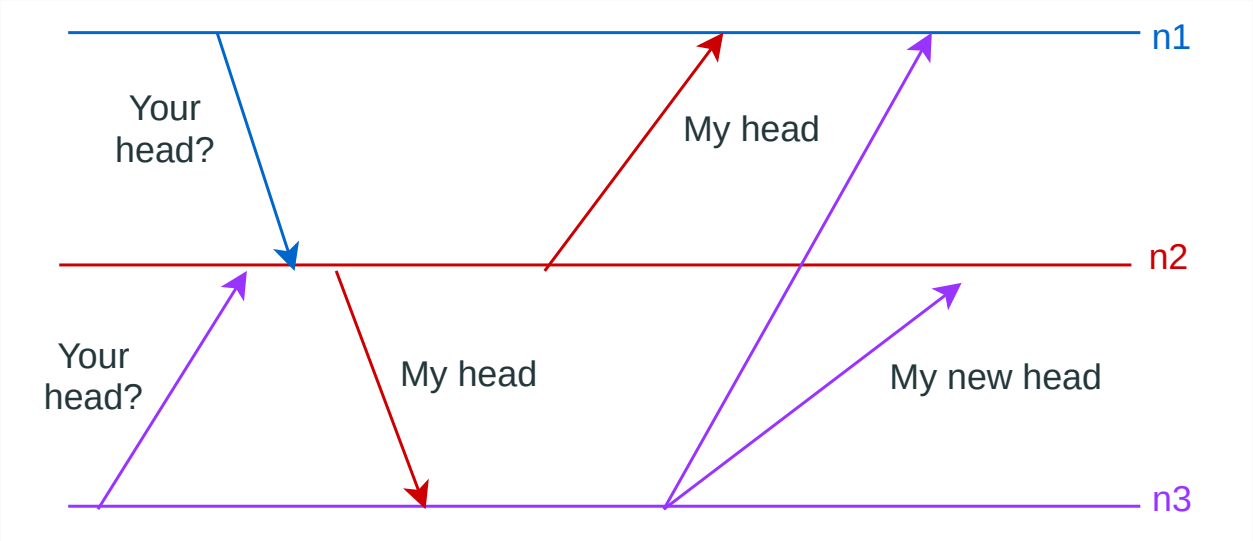
Journée scientifique Inria - Nomadic Labs

September 21, 2020

Formalising a Blockchain Protocol with a Self-amendmend Mechanism

Blockchain Protocols at a Glance

A Message passing protocol enabling a network to manage a replicated, append-only data structure (*a blockchain*).



Coordinate to reach an agreement on the blockchain content.

Blockchain Properties

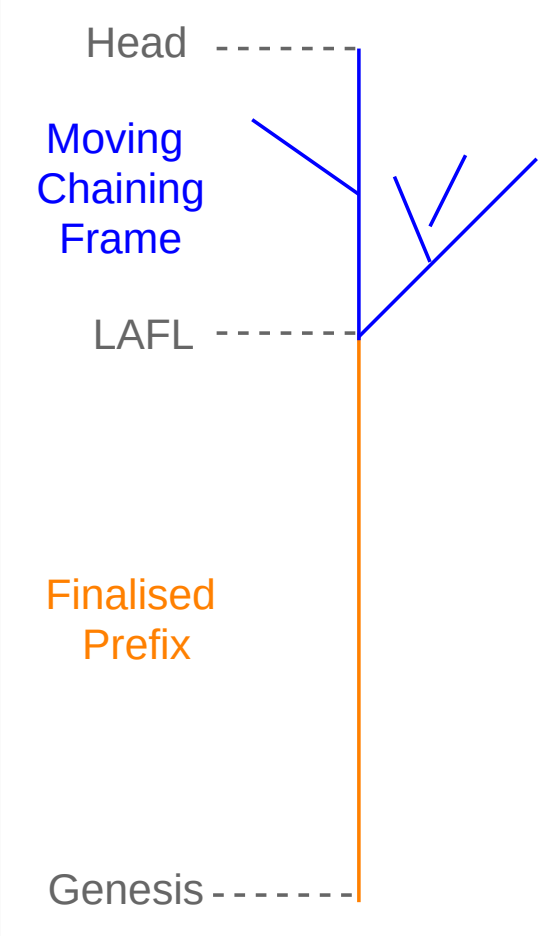
Eventual Consistency: All nodes will eventually share the same view of the blockchain.

- *Common Prefix*: Every node shares a common prefix of the eventual consistent view.
- *Chain Growth*: Each shared common prefix grows as new blocks are appended.

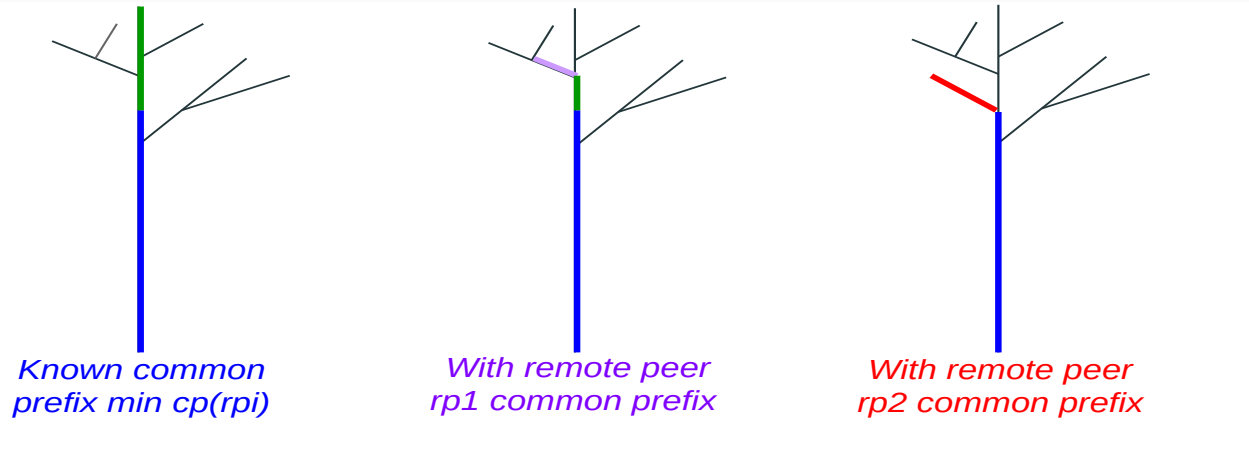
Node Blocktree Management

Block-chaining:

- Takes place in the moving chaining frame (latency absorption),
- Preserves chain integrity,
- It has *reached agreement*,
- It might become the new head.



Node Properties



Node common prefixes:

- A *peer common prefix* with each remote peer.
- The *known common prefix* with all remote peers.

Node chain growth: the node receives a new head from at least one of its remote peers.

Network Properties

Network properties are lift from node's ones in a suitable *Execution model*: communication model and scheduling.

- *Common Prefix*: of every node's known common prefix.
- *Chain Growth*: New block injection ensures that at least one node will eventually have a new head to advertise.

Beyond a network of honest nodes:

How to model faulty, Byzantine nodes?
Rational behaviors?
Which consistency criteria?

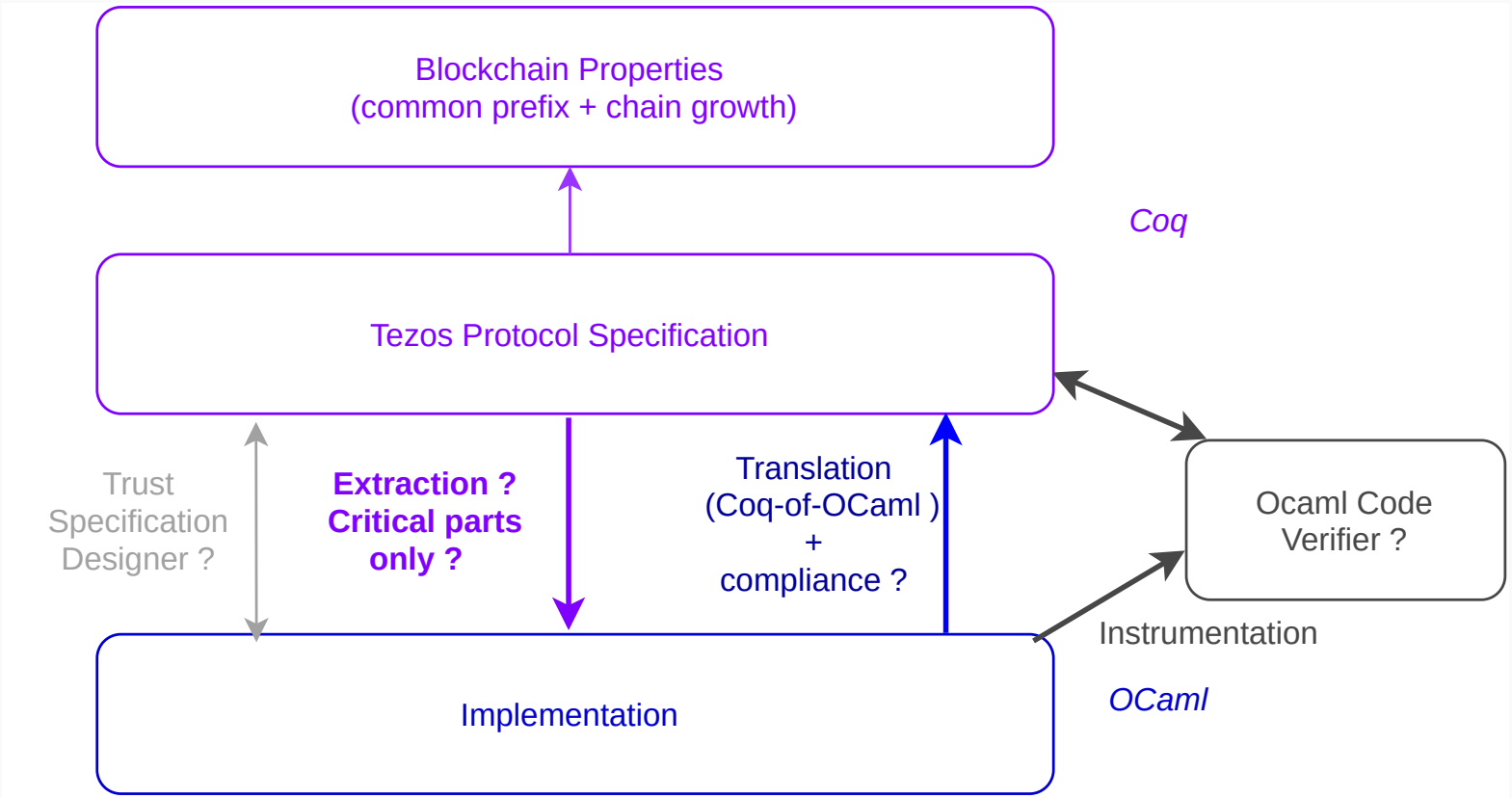
Modeling Self-amendmend

- Remaining a cutting-edge blockchain while preventing hard forks.
- Blockchain protocol is parametric and not generic.
- Economic protocol and switches of economic protocol.
- *Abstract Economic Protocol* models an economic protocol, exposing relevant properties for Common Prefix and Chain Growth.

How to Model economic protocol switches?
How does it impact global reasonning?

Formal Verification in a Development Process

Implementation Verification



Looking for a formal verification process that is mantainable and enabling software update verification.