5th of June 2023

Master's Thesis Defence

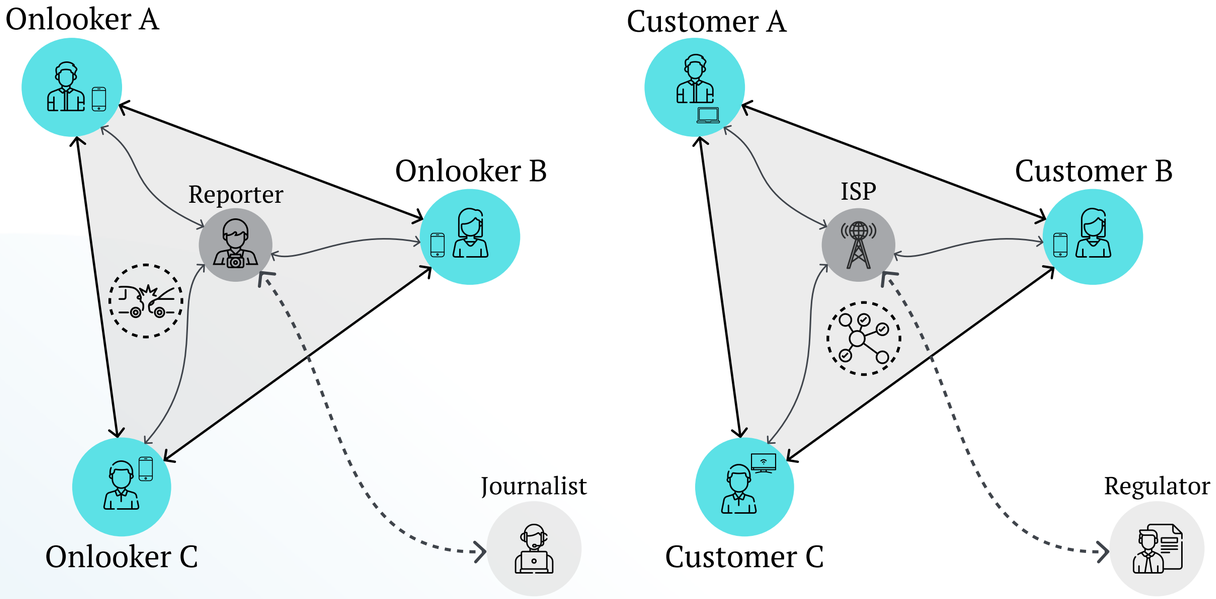
Towards Decentralized Proof-of-Location

Eduardo Ribas Brito
Supervised by Ulrich Norbisrath

UNIVERSITY OF TARTU
Institute of Computer Science

Location-based Authentication/Authorization

In Adversarial Environments



Thesis Outline

1. The Proof-of-Location Paradigm
2. The Evolution of PoL Systems
3. A Novel Decentralized Protocol
4. A Proof-of-Concept Implementation

SMART CITIES

AUGMENTED DEMOCRACY

LOCATION PROVENANCE

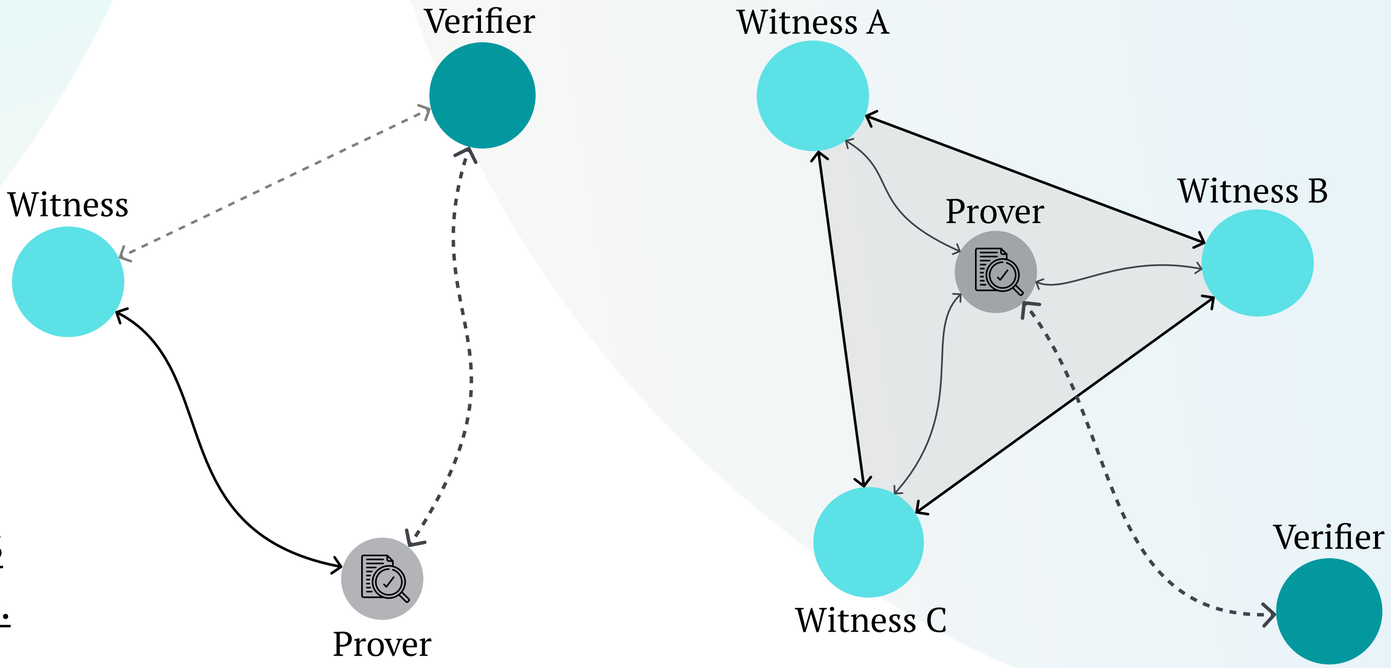
INTERNET TRANSPARENCY

DIGITAL INTEGRITY

SOCIAL ACCOUNTABILITY

A digital Proof-of-Location

Is an electronic certificate that attests one's position in both space and time.



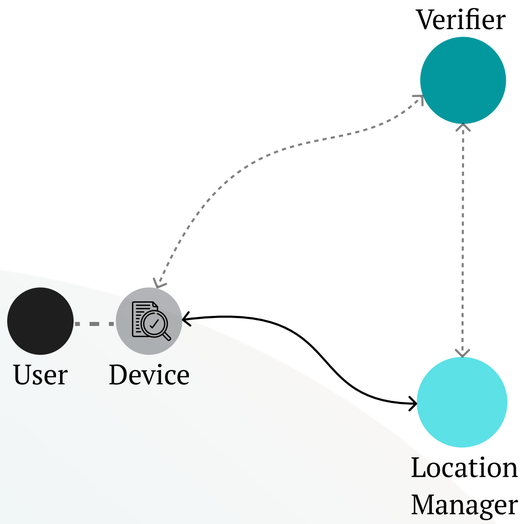
Centralized Proof-of-Location

Decentralized Proof-of-Location

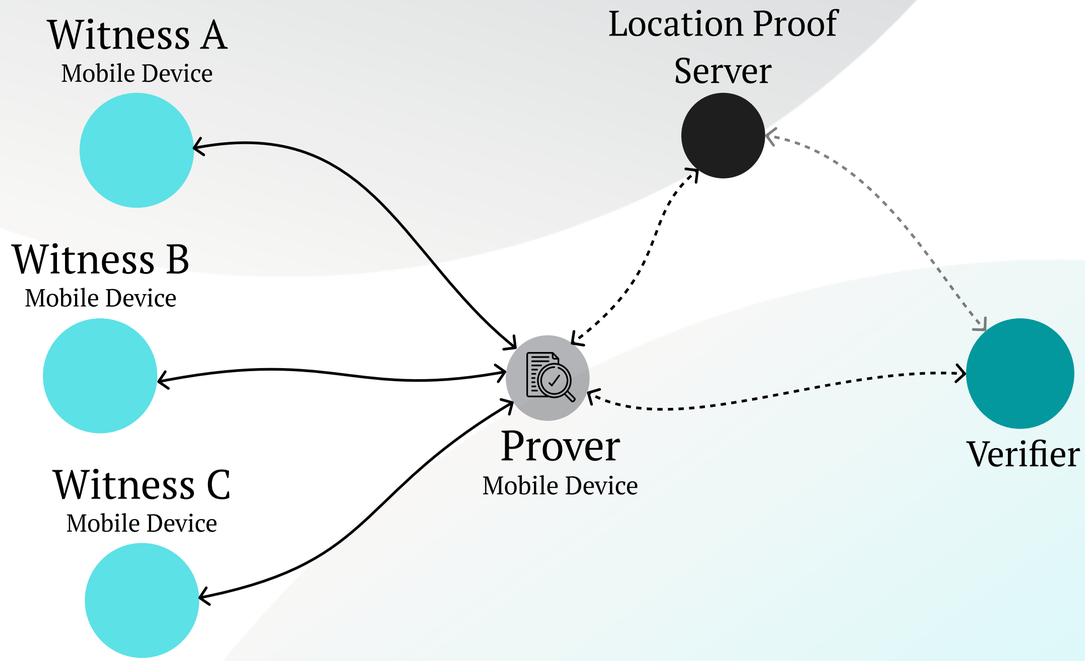
short-range, synchronous communication

long-range, asynchronous communication

The evolution of Location Proof Systems

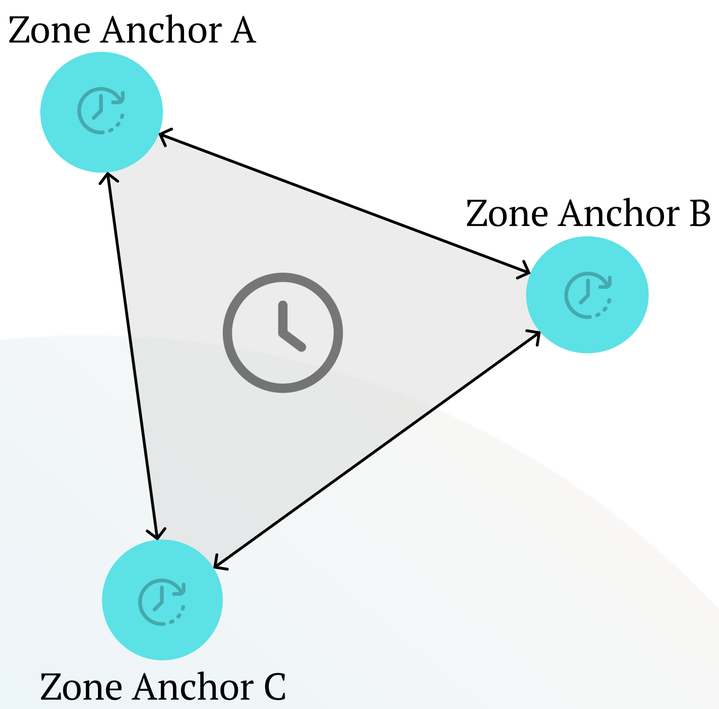


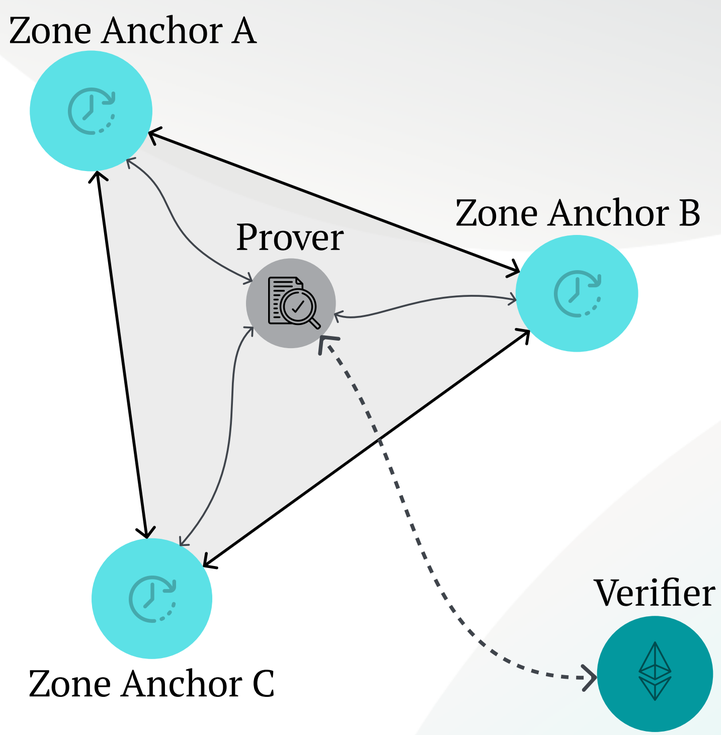
Trusted and Centralized Architectures



Progressively Distributed Systems

The evolution of Location Proof Systems



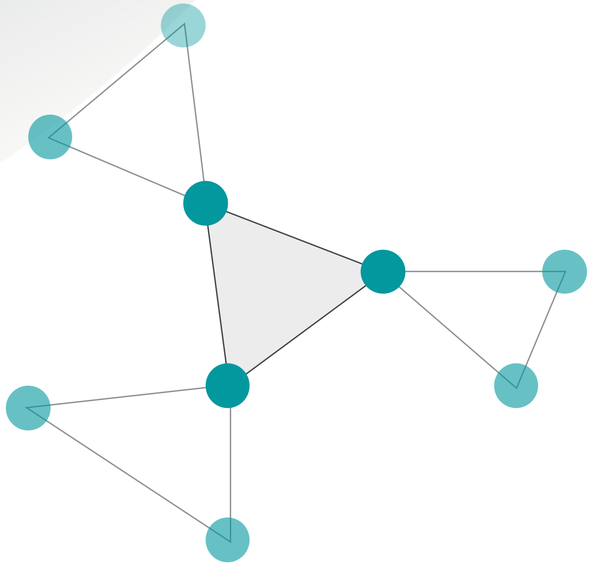


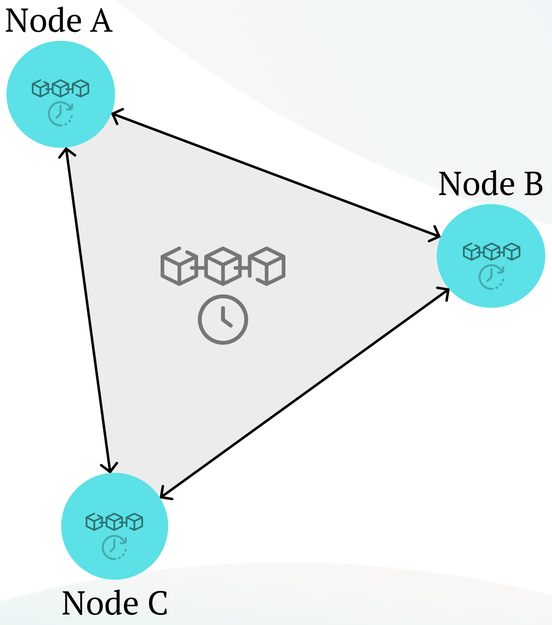
Considered secure if:

- Complete
- Spatio-temporally sound
- Non-transferable

Decentralized and Trustless Protocols

Space Synchronization + Time Synchronization





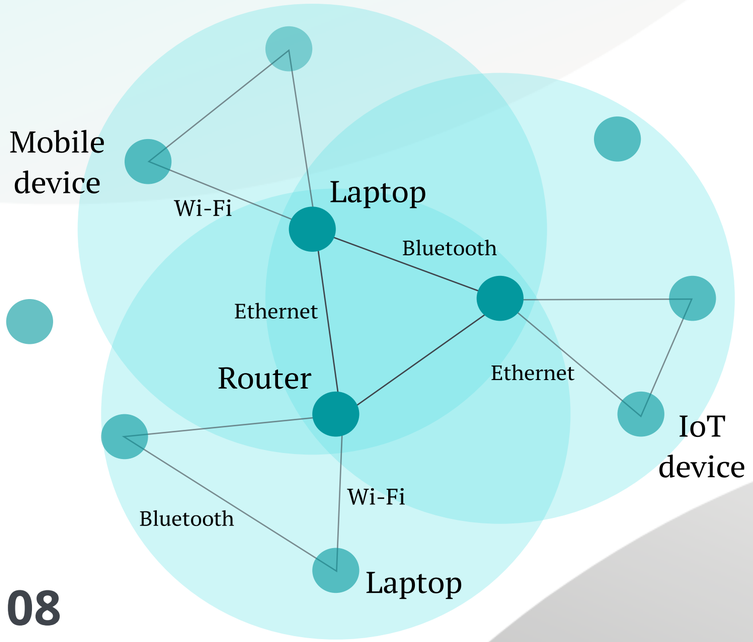
=

Trustless Proof-of-Location

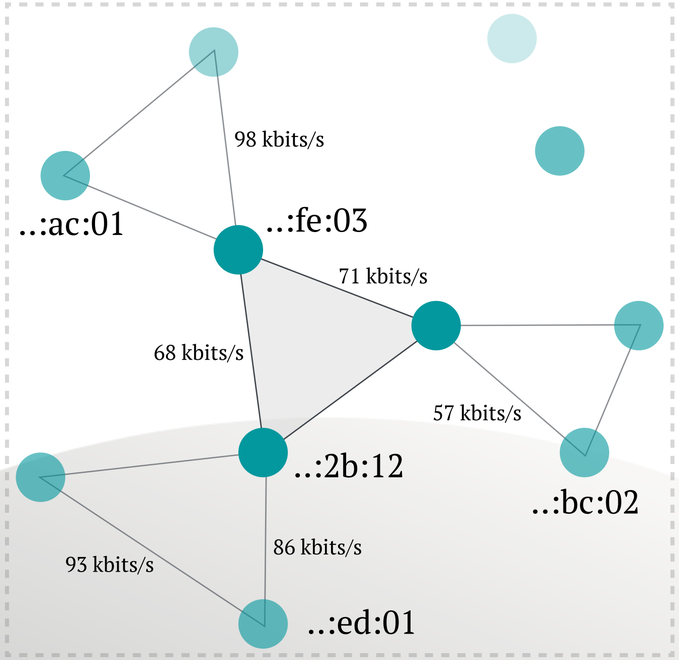
Dynamic and Non-Hierarchic Mesh Networks

Layer 2 Routing Protocols

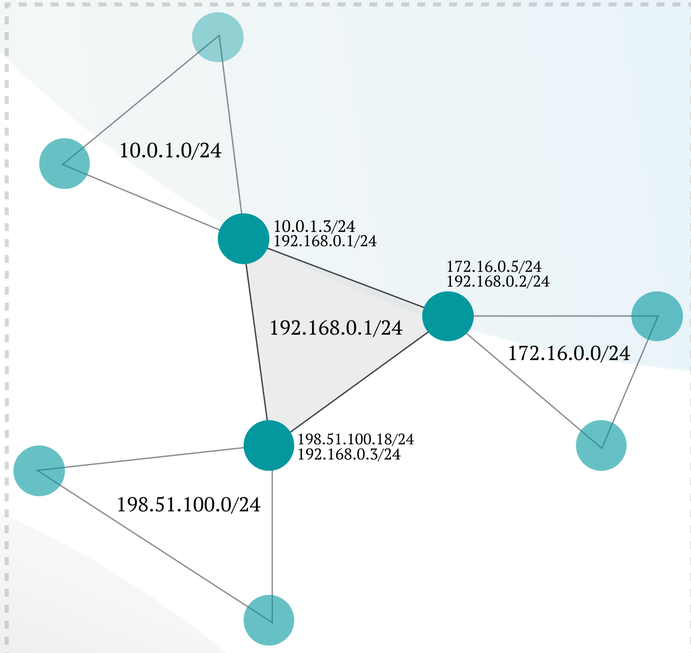
Peer-to-Peer Short-ranged Communication



Neigbourhood Discovery and Ranking

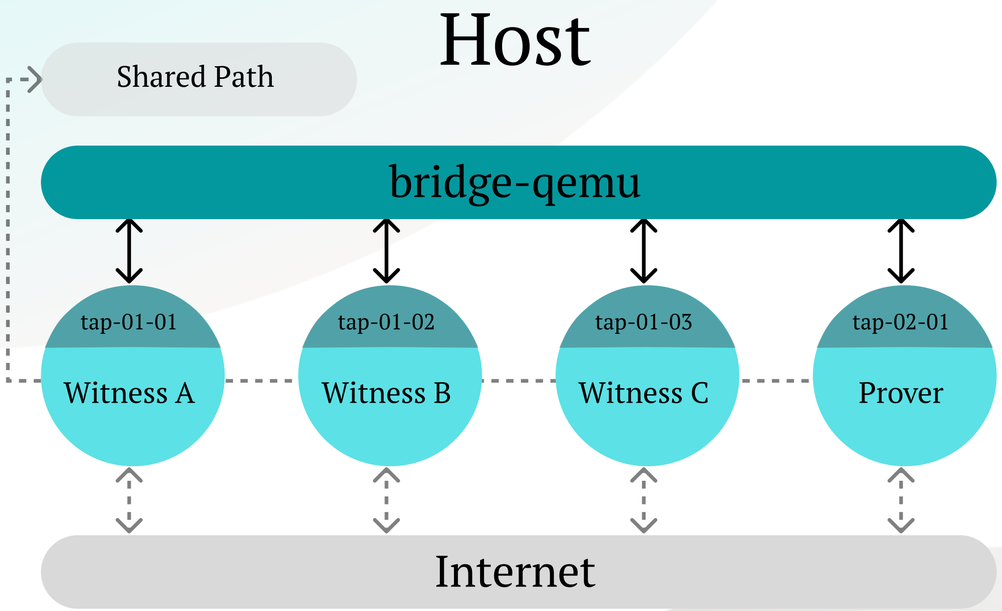


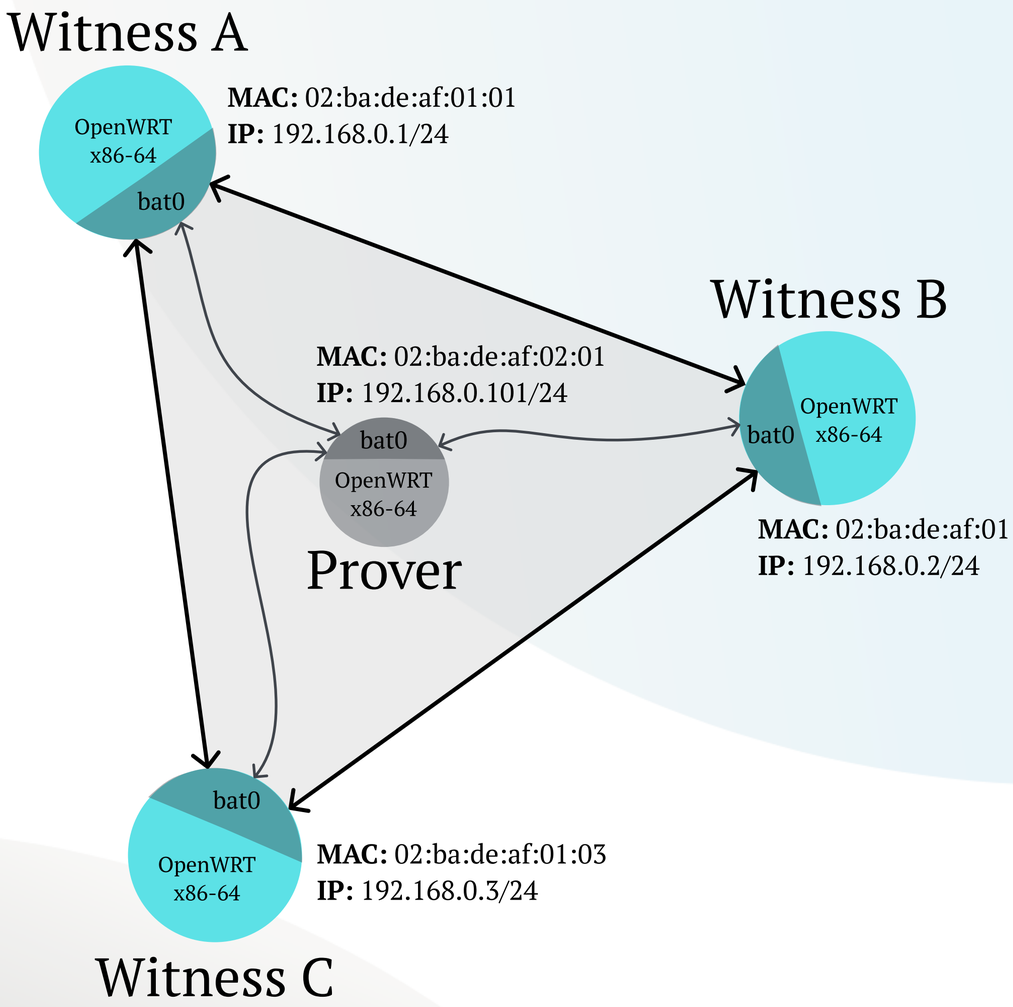
Zone Establishment and Affinity



Testbed Setup and Network Architecture

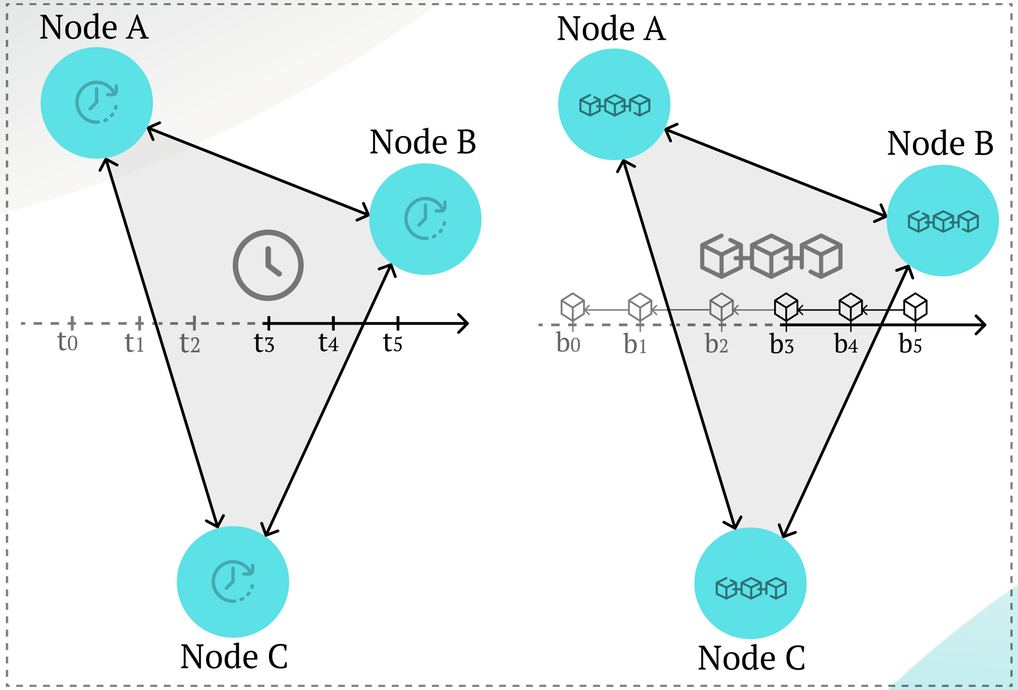
OpenWrt, QEMU, batman-adv



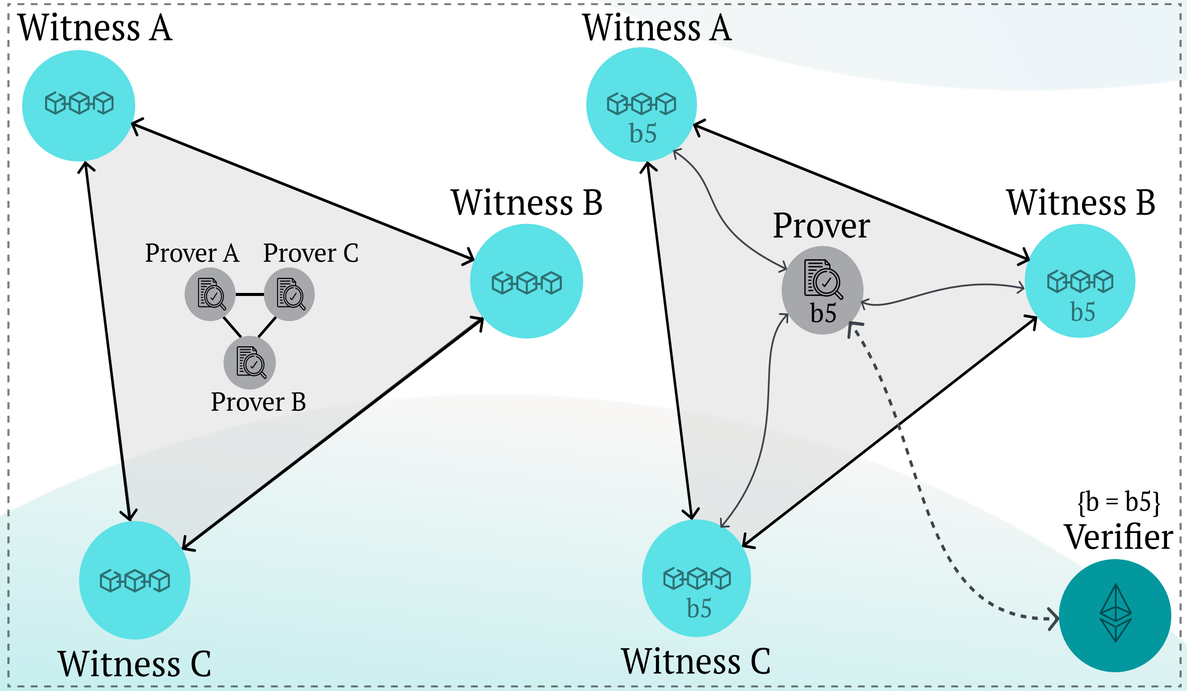


Turing-Complete Clock Synchronization

Permissionless Consensus Mechanisms



Zone-relative
Time Consciousness

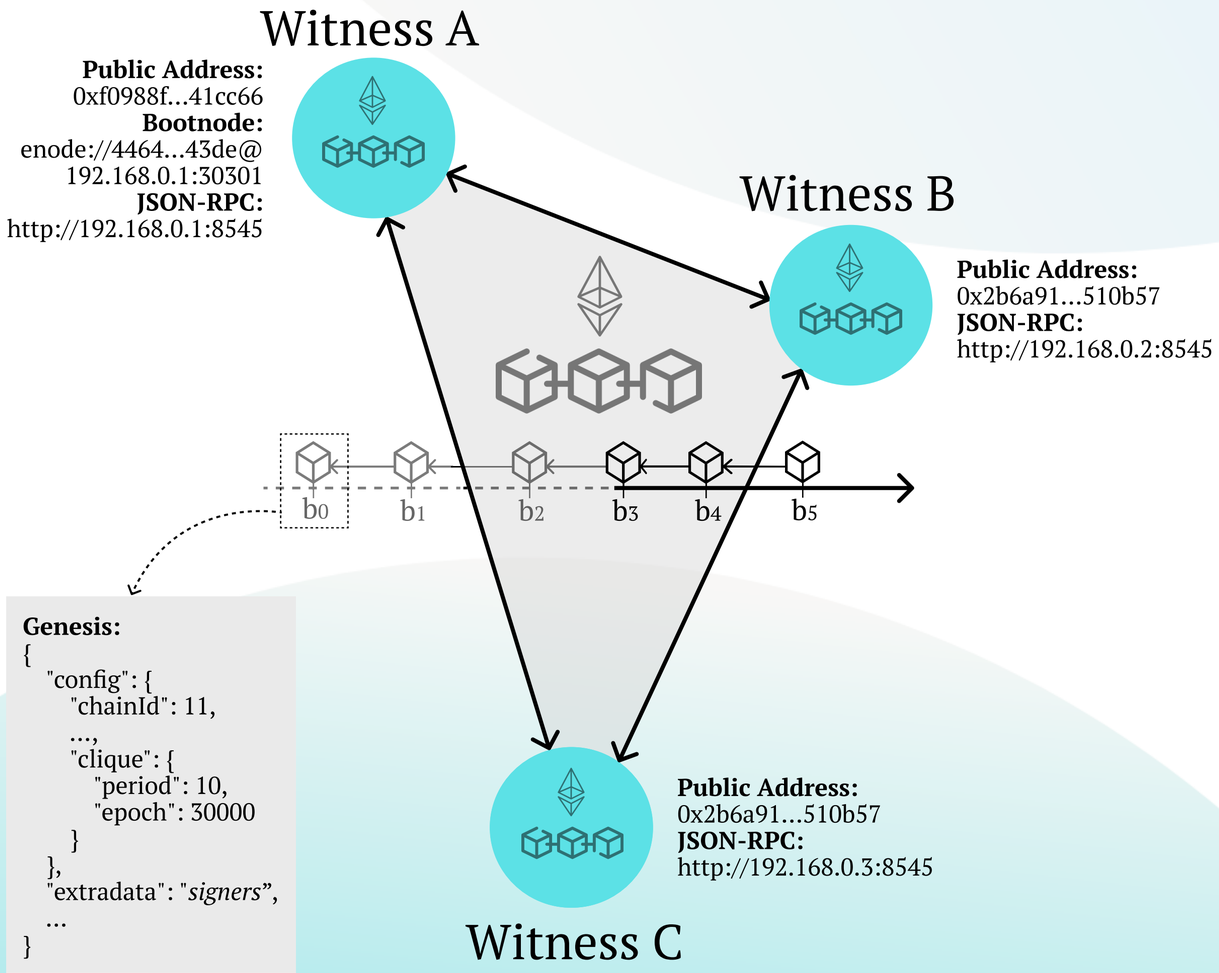


Turing-Complete
Smart Contracts

Practical Permissionless Consensus

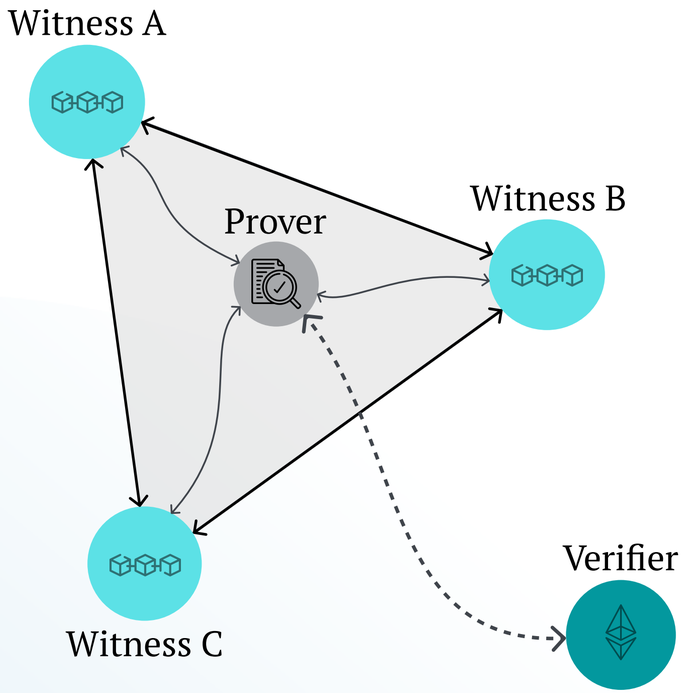
Ad-hoc Ethereum Network

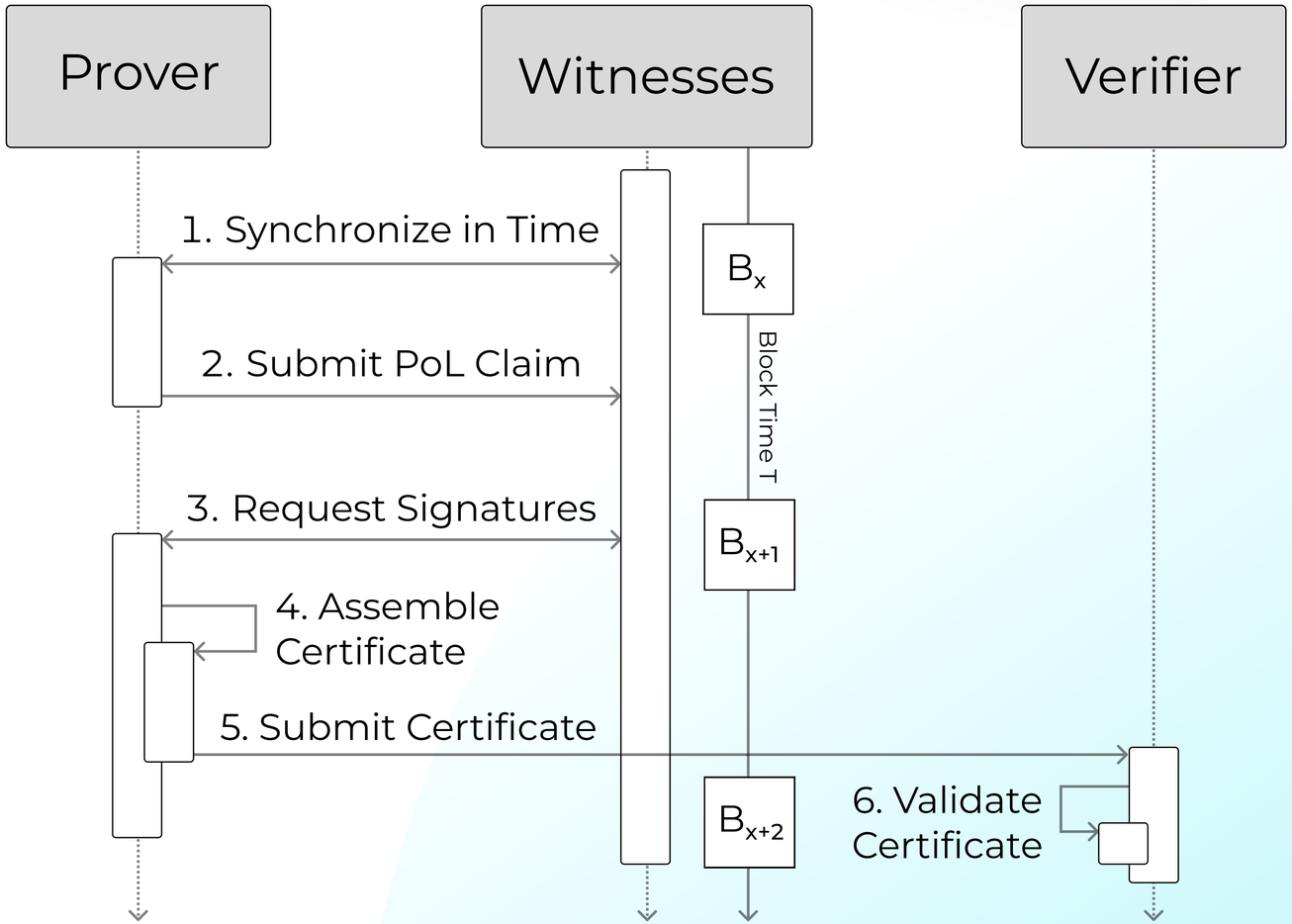
1. Consensus protocol:
   - Proof-of-Work vs Proof-of-Authority
2. The block time:
   - fixed vs dynamic
3. Initialization and discovery:
   - Genesis file and bootnodes
4. Smart contracts:
   - Solidity and EVM



Proof Generation and Verification

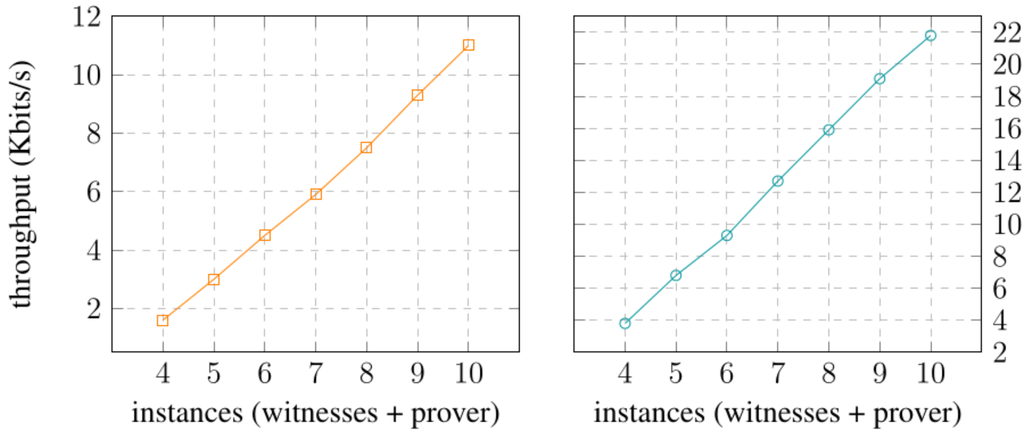
Prover & Verifier Processes





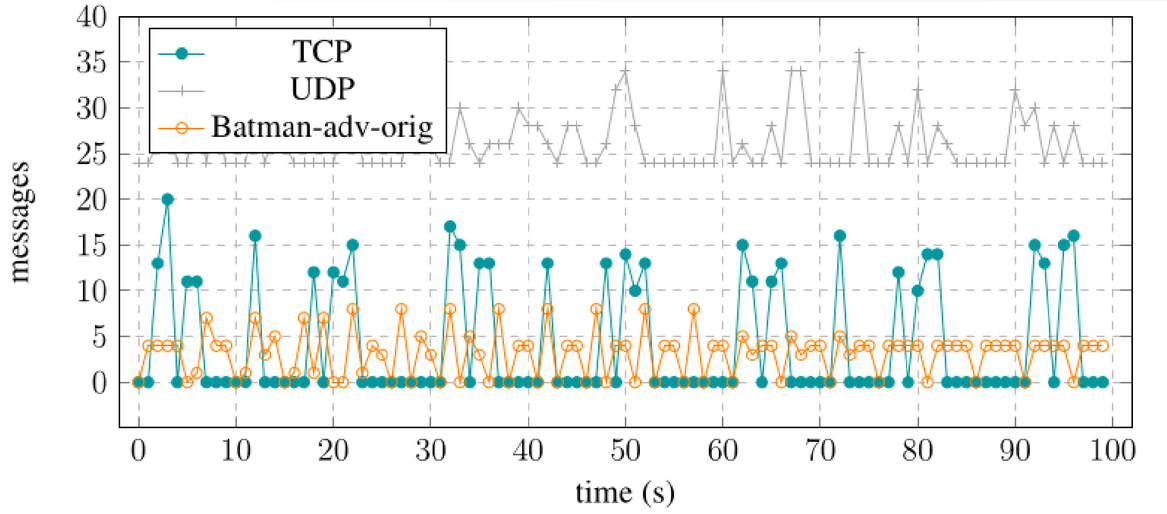
Performance Measurements

Protocols throughput

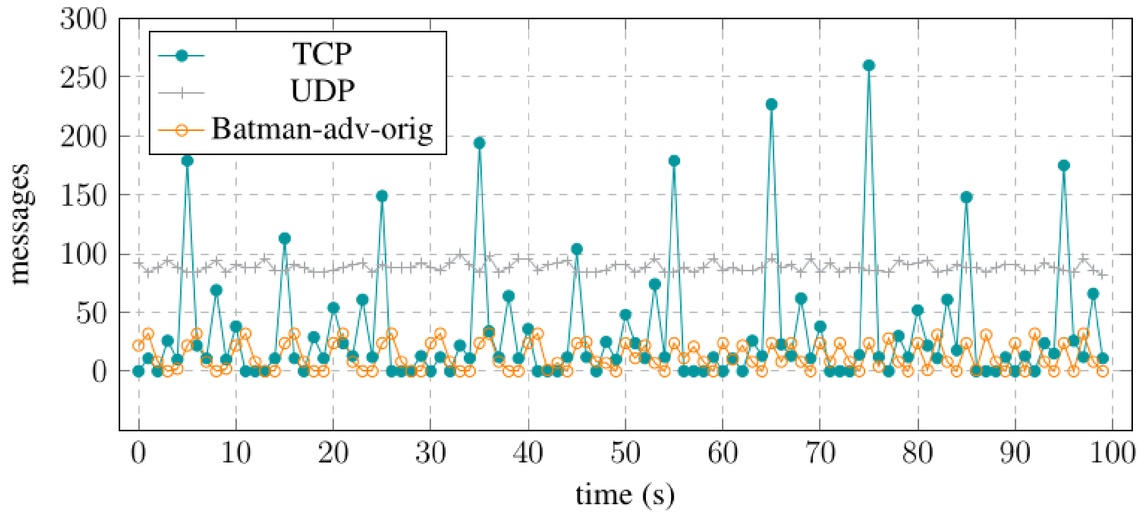


(a) Batman-adv traffic throughput.

(b) IPv4 traffic throughput.



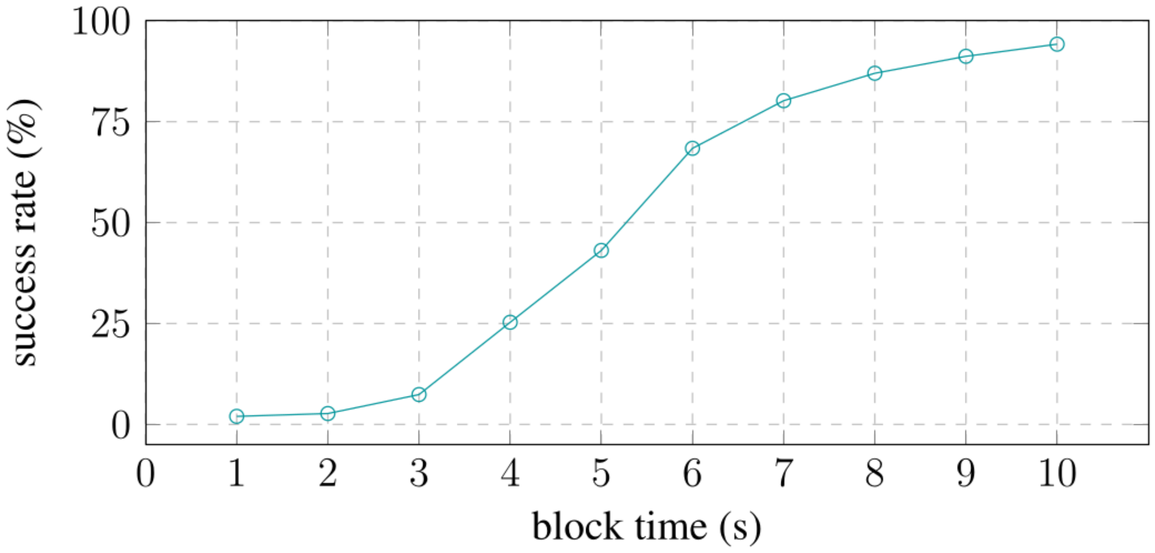
(a) 4 instances.

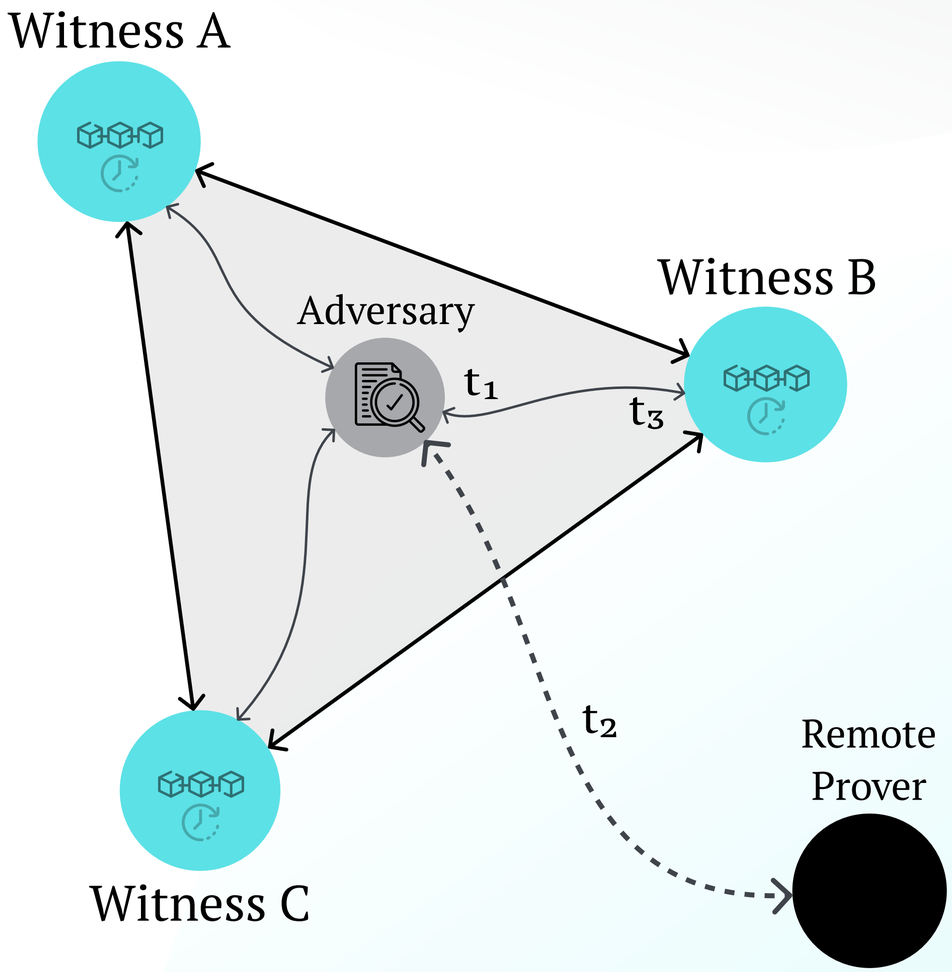


(b) 8 instances.

Success Rate and Attack Vectors

Block time and Proxy attacks





Summary and Future Work

1. The Proof-of-Location Paradigm

2. The Evolution of PoL Systems

3. A Novel Decentralized Protocol

4. A Proof-of-Concept Implementation

IDENTITY MANAGEMENT SYSTEMS

SMART CONTRACTS

INCENTIVE MECHANISMS

CONSENSUS PROTOCOLS

PRIVACY PRESERVING TECHNOLOGIES

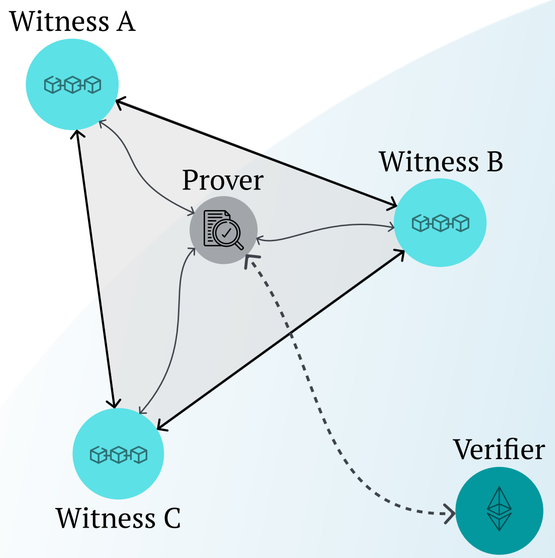
PHYSICAL DEPLOYMENT

5th of June 2023

Master's Thesis Defence

Towards Decentralized Proof-of-Location

Reality is merely an illusion,
albeit a very ~~persistent~~ consensual one.
- Albert Einstein
Somewhere, at some point in time



Eduardo Ribas Brito
Supervised by Ulrich Norbisrath

UNIVERSITY OF TARTU
Institute of Computer Science

Appendix

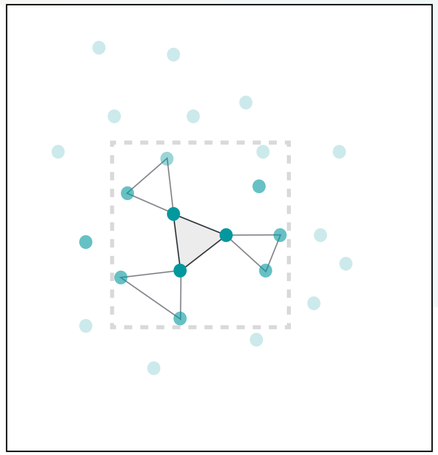
Overview

Protocol Fundamentals

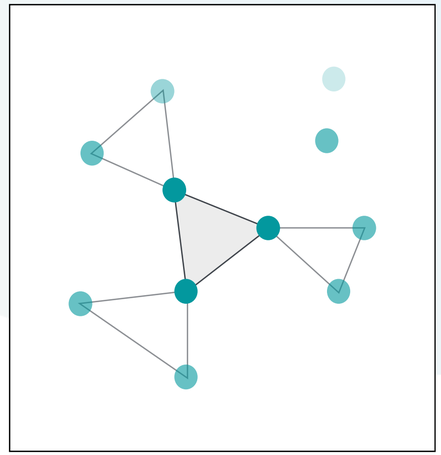
From a dynamic mesh topology, towards the ultimate goal of achieving Absolute Proof-of-Location.

A. Mesh Network

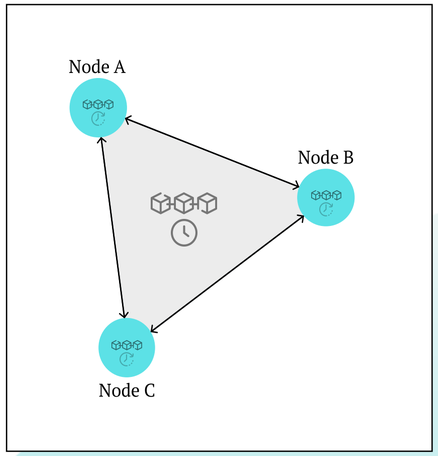
B. Zone Discovery



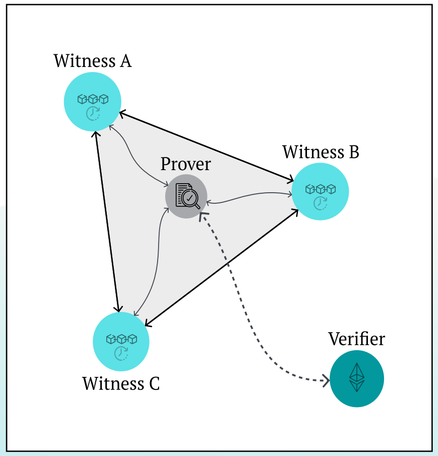
C. Zone Affinity



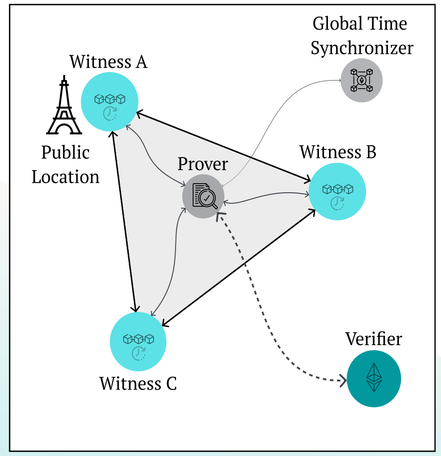
D. Zone Synchronization



E. Relative Proof-of-Location



F. Absolute Proof-of-Location

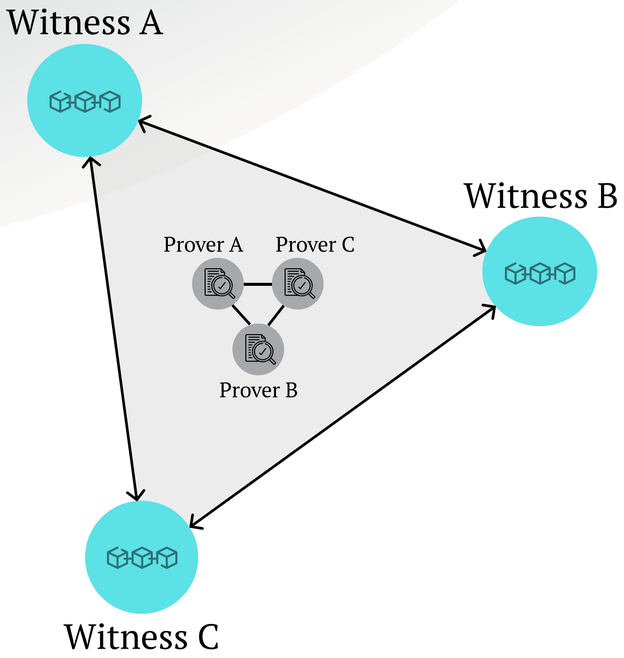


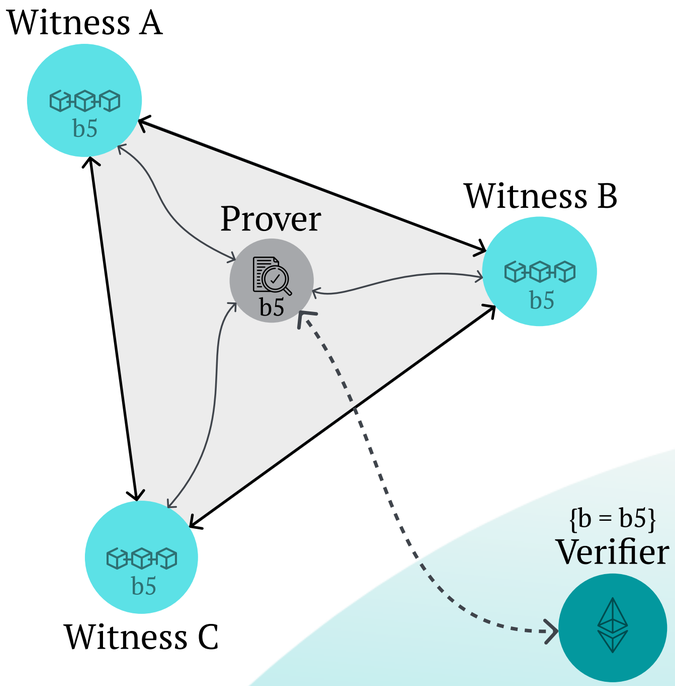
short-range, synchronous communication

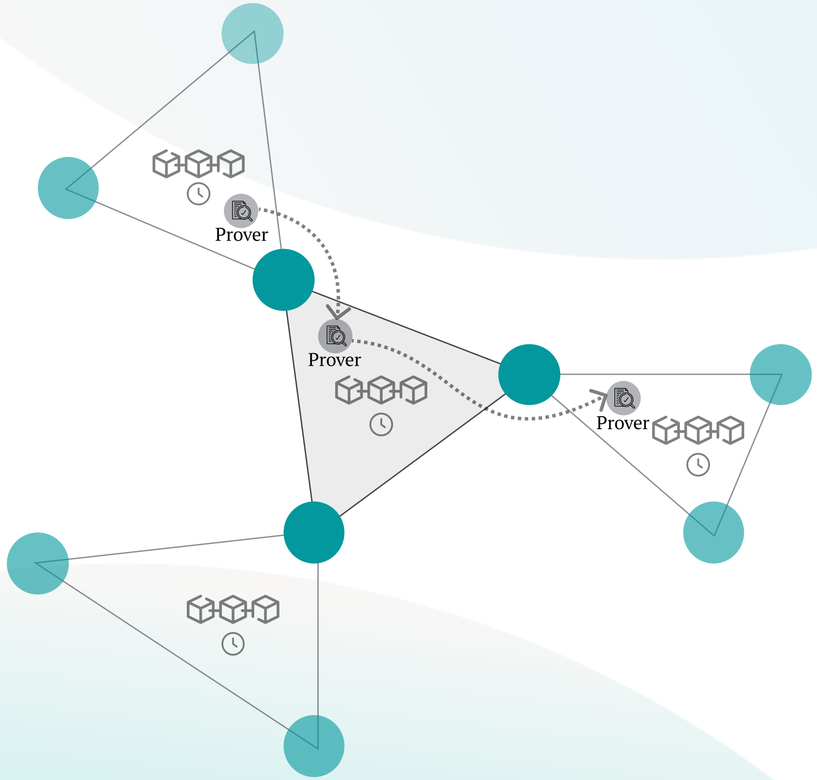
long-range, asynchronous communication

Smart Contracts

Turing-Completeness use cases

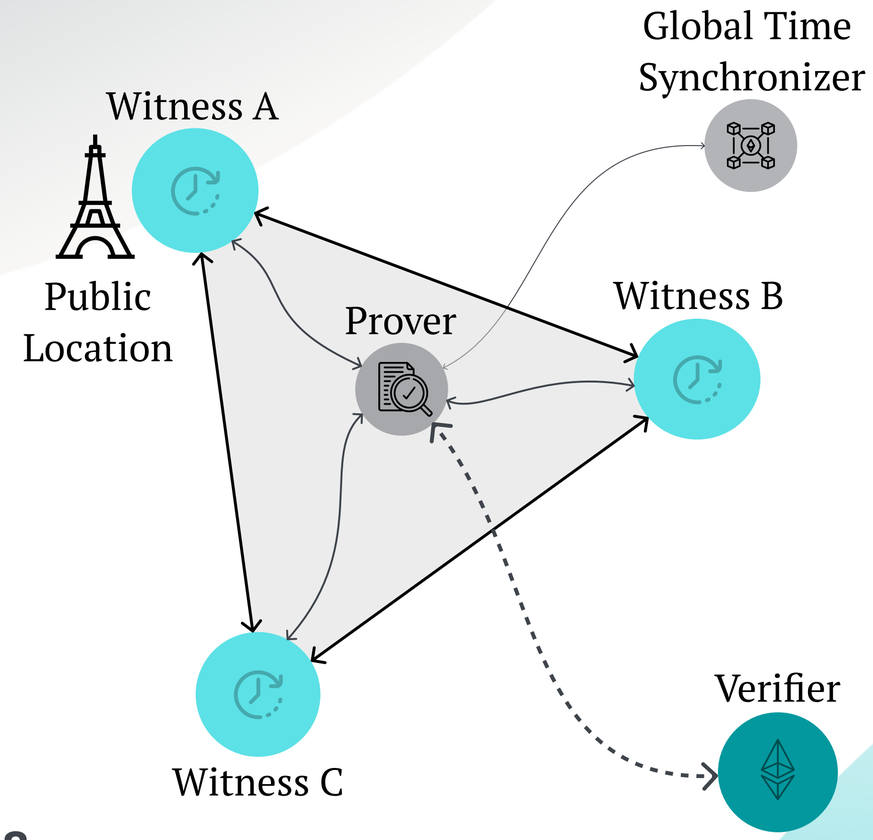






Absolute Proof-of-Location

From Relative Proof-of-Location



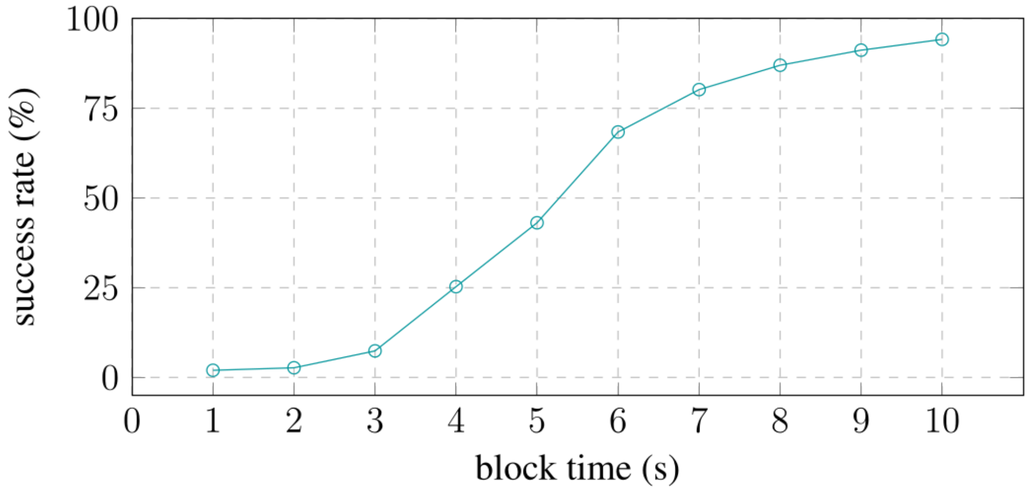
A Proof-of-Location certificate to be spatially and temporally acknowledged by any other node outside the zone needs:

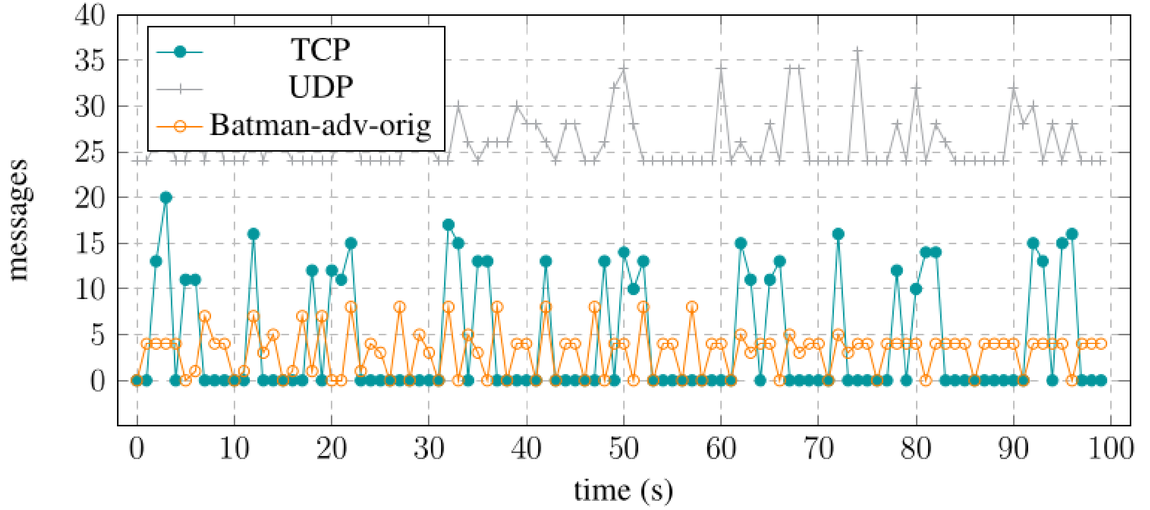
- Global Time Synchronization Protocol
  - NTP, PTP, Public Blockchain?
  - Trusted timestamping?
- Global Positioning System
  - GPS, crypto-spatial coordinates?

Measurements

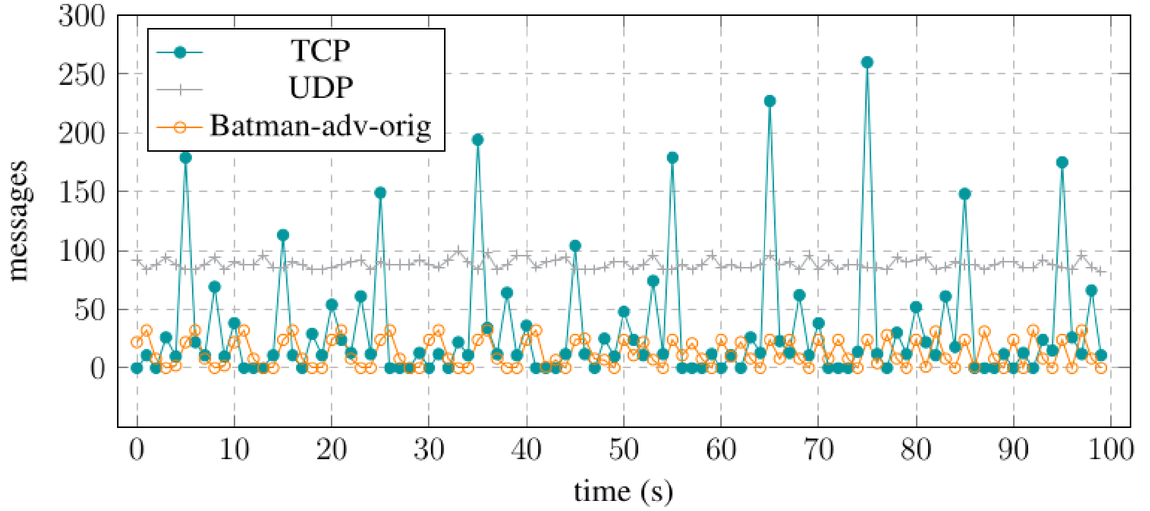
Blockchain Activity & Success Rate

1. The interval time between blocks matches the higher peaks of TCP traffic, while the UDP traffic is more evenly distributed.
2. A more permissive block time allows for a lower number of invalid certificates, but also for a higher probability of witnessing malicious activity.



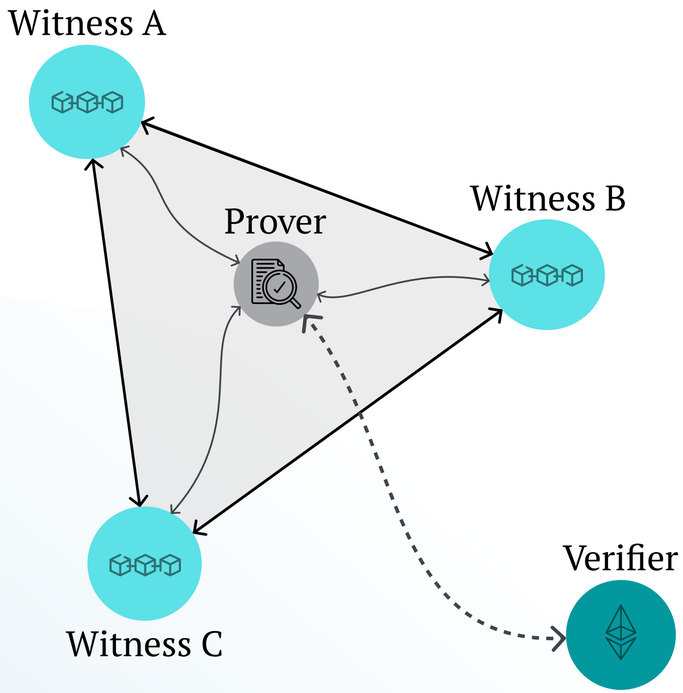


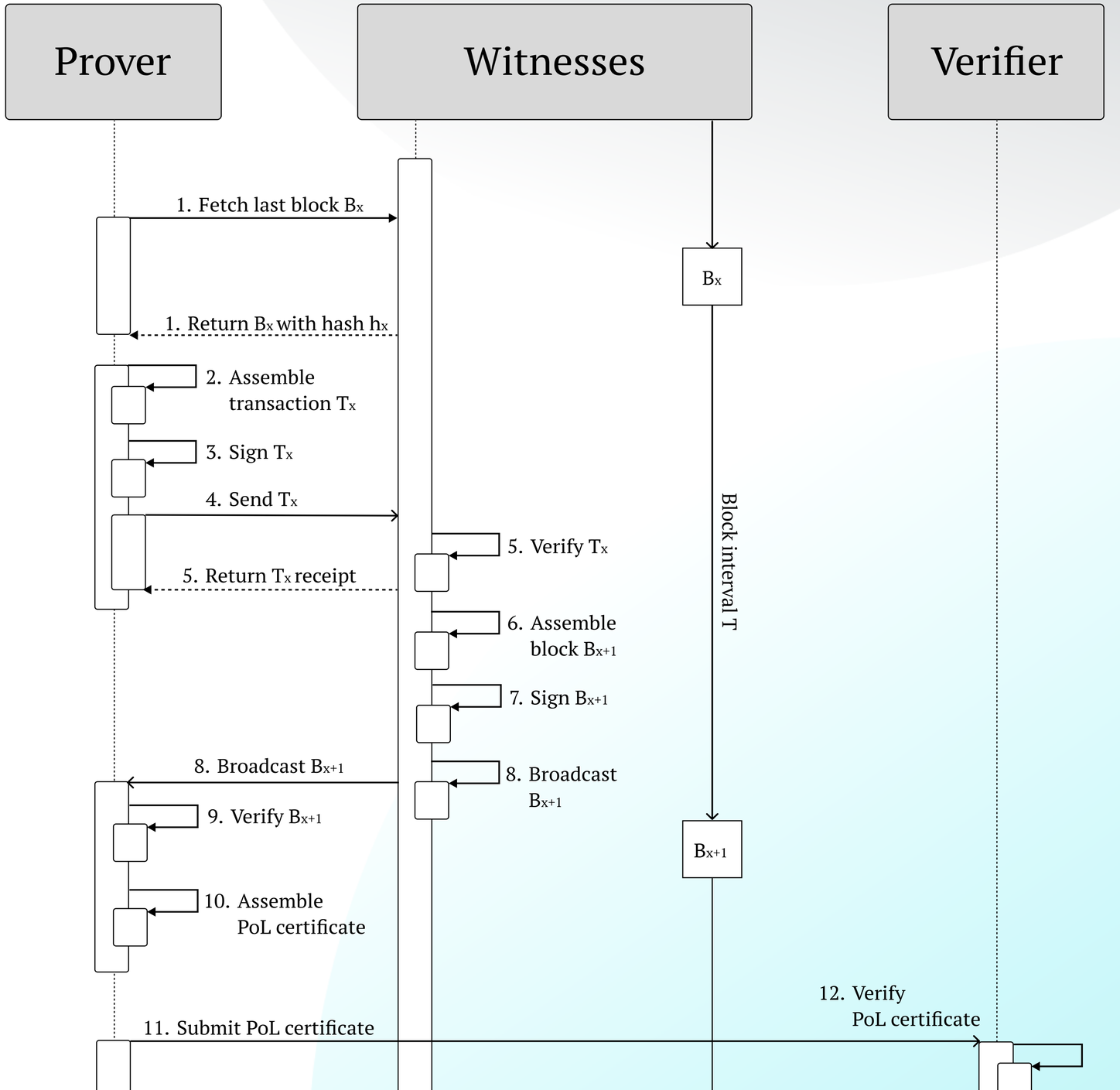
(a) 4 instances.



(b) 8 instances.

Proof Generation and Verification





Future Work

1. **Zone Establishment and Affinity:**
    a. More effective identity management systems and crypto-economic incentives
2. **Consensus Mechanisms:**
    a. From deterministic-finality Byzantine fault-tolerant algorithms to probabilistic finality consensus mechanisms
3. **Smart Contracts:**
    a. Making full use of the system's Turing completeness for more complex logic
4. **Protocol Extensibility:**
    a. Integration of privacy preserving mechanisms, such as zero-knowledge proofs
5. **Physical Deployment:**
    a. And the evaluation of the performance in real-world scenarios