16th May 2023

Distributed Systems Seminar

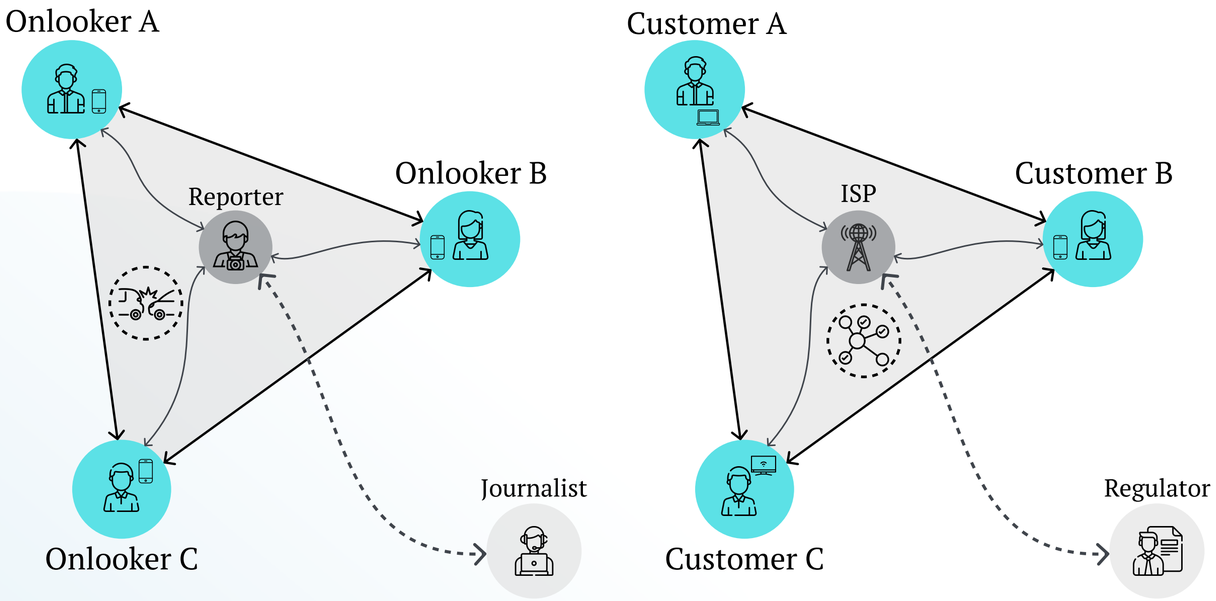
Towards Decentralized Proof-of-Location

Eduardo Ribas Brito
Supervised by Ulrich Norbisrath

UNIVERSITY OF TARTU
Institute of Computer Science

Location-based Authentication/Authorization

In Adversarial Environments

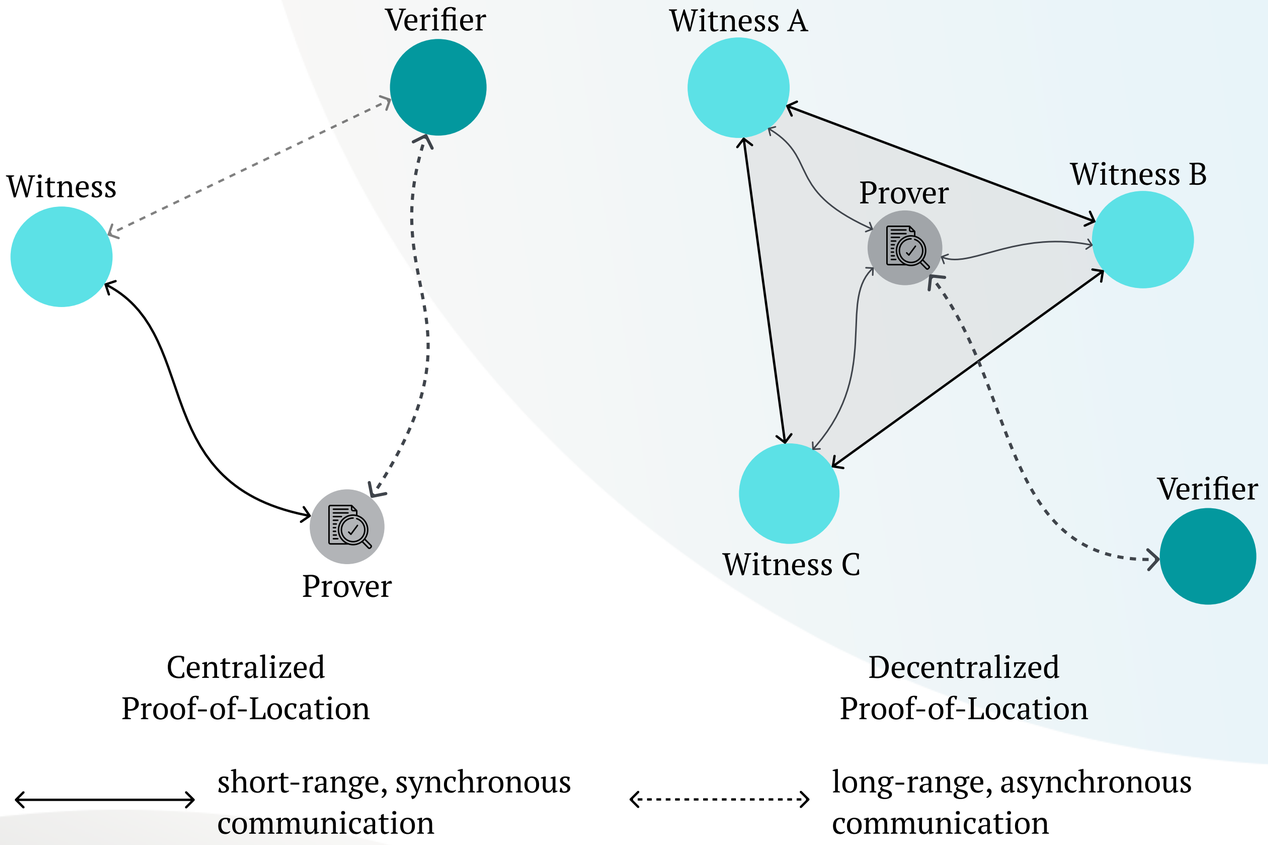


A digital Proof-of-Location

Is an electronic certificate that attests one's relative position in both space and time [1].

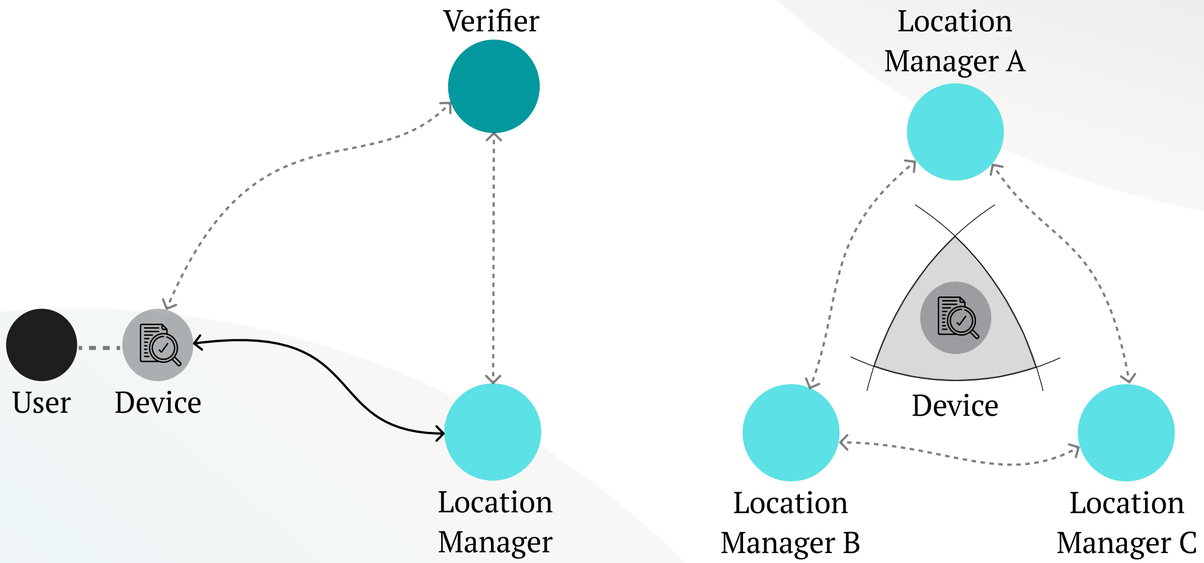
Considered secure if:

- **Complete**
- **Spatio-temporally sound**
- **Non-transferable**



[1] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, "Blockchain-based proof of location"

The evolution of Location Proof Systems



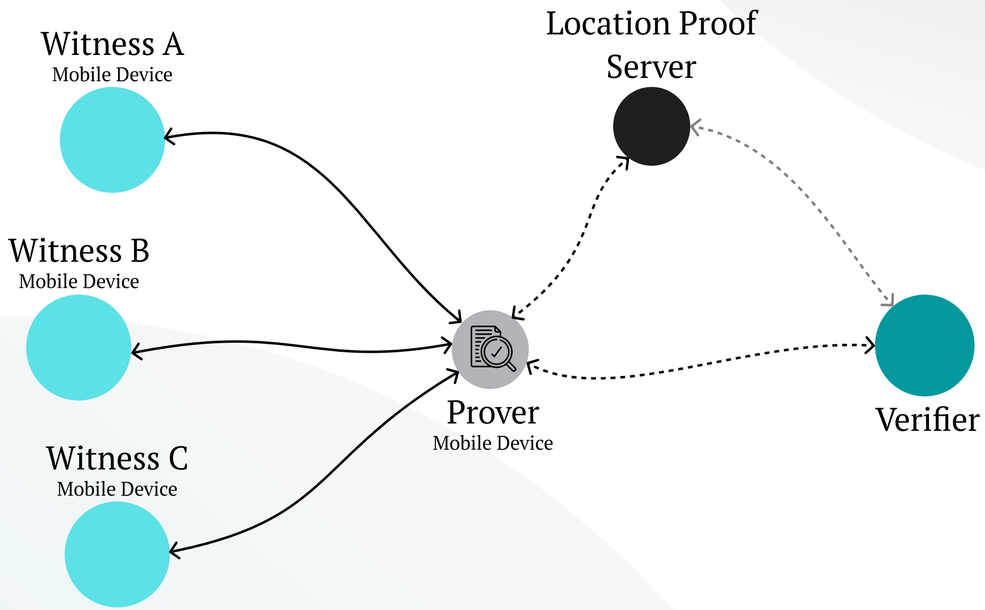
Trusted and Centralized Architectures

A location-proving system:

- By proximity, with integrity and privacy guarantees.
- Assuming
  - a trusted verifier, device and location manager,
  - an untrusted user.
- Using round-trip and signal propagation latency metrics.

[2] Brent R. Waters and Edward W. Felten, "Secure, Private Proofs of Location."

The evolution of Location Proof Systems



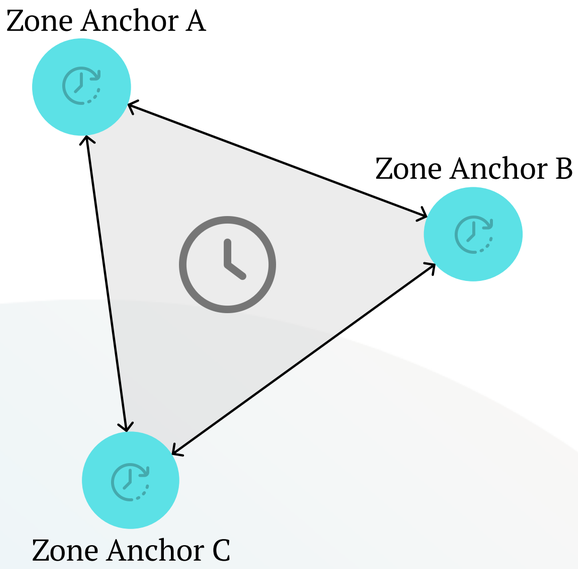
Progressively Distributed Systems

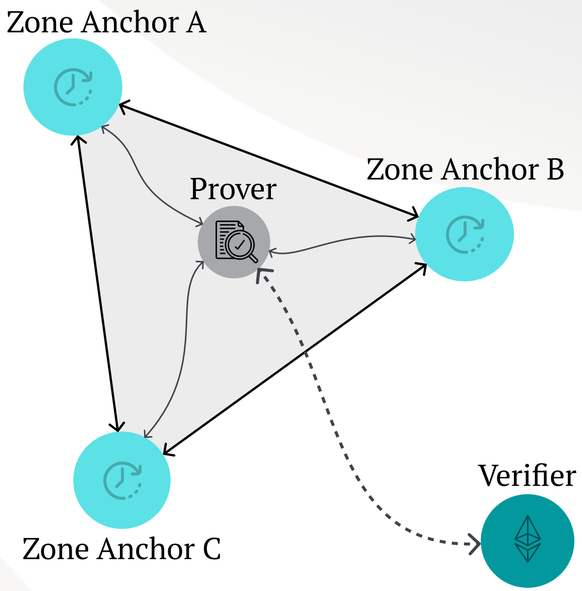
A privacy-aware distributed protocol:

- Using Bluetooth-enabled mobile devices for proof generation.
- Assuming a trusted prover, verifier, and witnesses.
- Following a user-centric privacy model through statistical pseudonym changing.
- Storing location-proof records in a trustless manner.

[3] Z. Zhu and G. Cao, “Applaus: A privacy-preserving location proof updating system for location-based services”

The evolution of Location Proof Systems





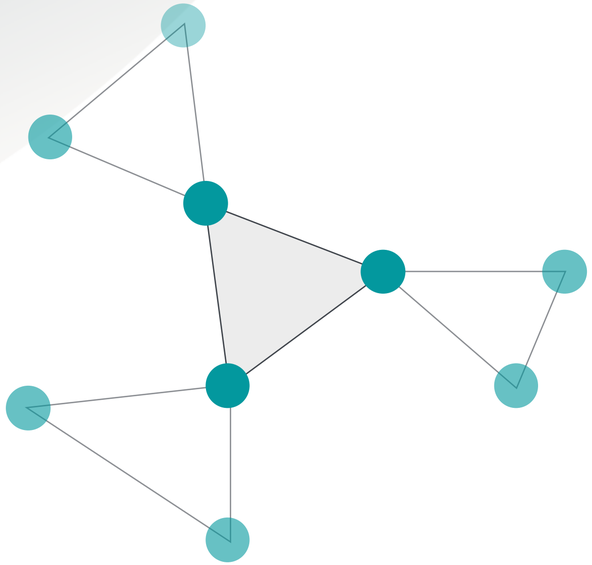
A decentralized protocol:

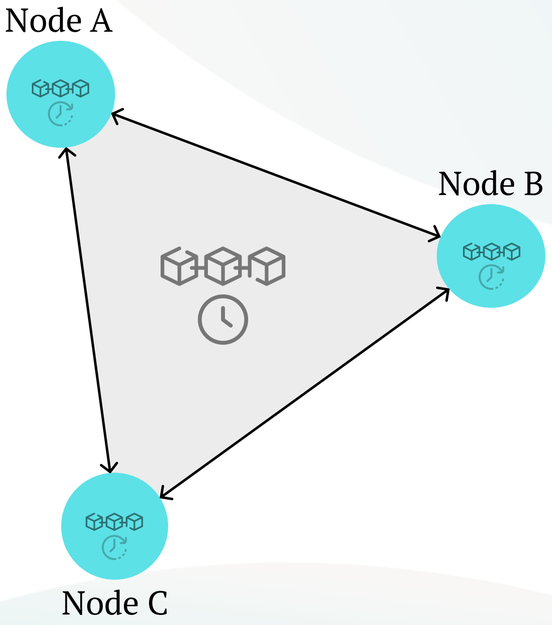
- Based on dynamic clock synchronization for trustless, spatio-temporally sound location services.
- Including token-curated registries, and crypto-economic incentives.
- Aims to create a consensus-driven map of the world.

Decentralized and Trustless Protocols

[4] R. J. King, “Foam: The importance of time synchronization.”

Space Synchronization + Time Synchronization





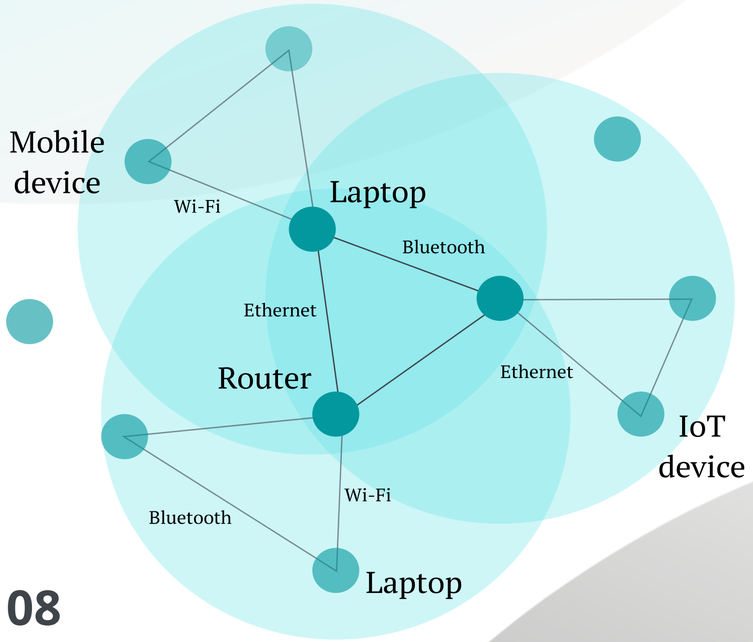
=

Trustless Proof-of-Location

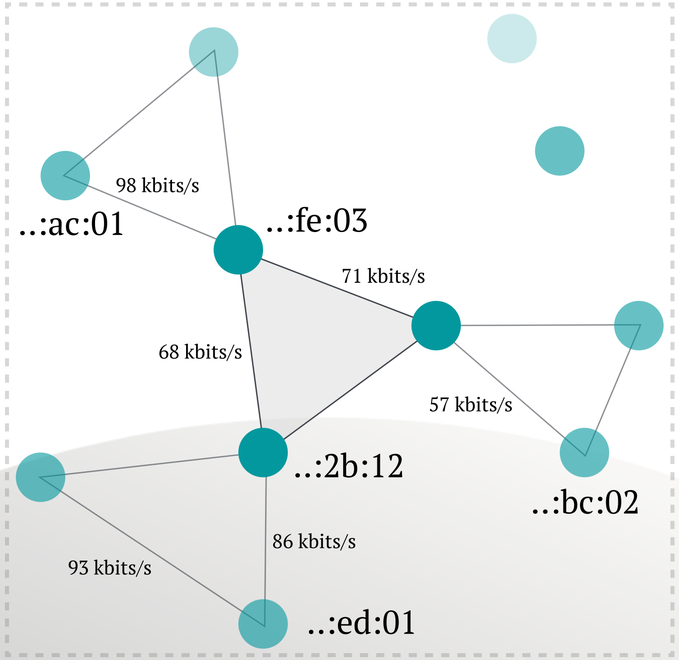
Dynamic and Non-Hierarchic Mesh Networks

Layer 2 Routing Protocols

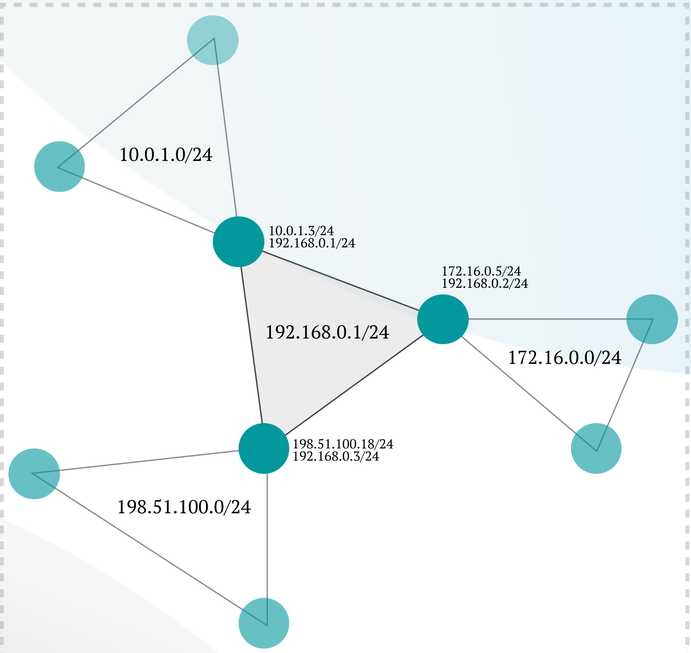
Peer-to-Peer Short-ranged Communication



Neigbourhood Discovery and Ranking

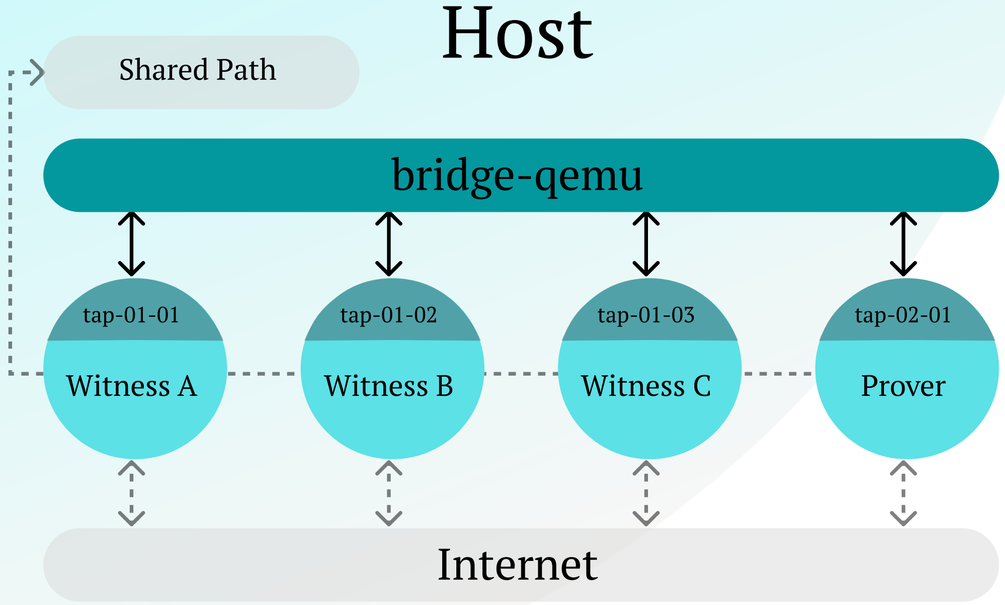


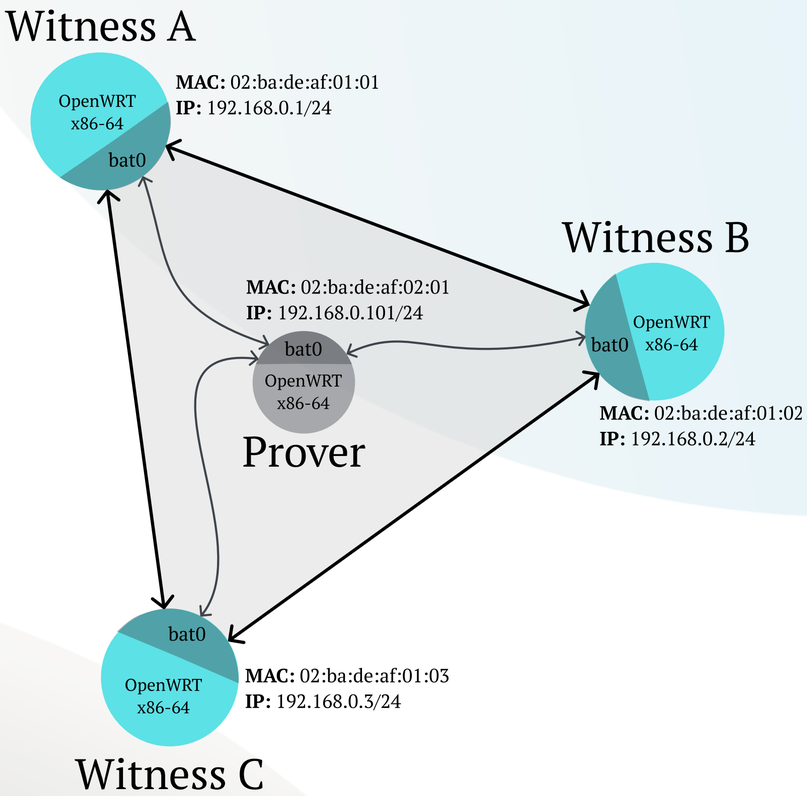
Zone Establishment and Affinity



Testbed Setup and Network Architecture

OpenWRT, QEMU, batman-adv

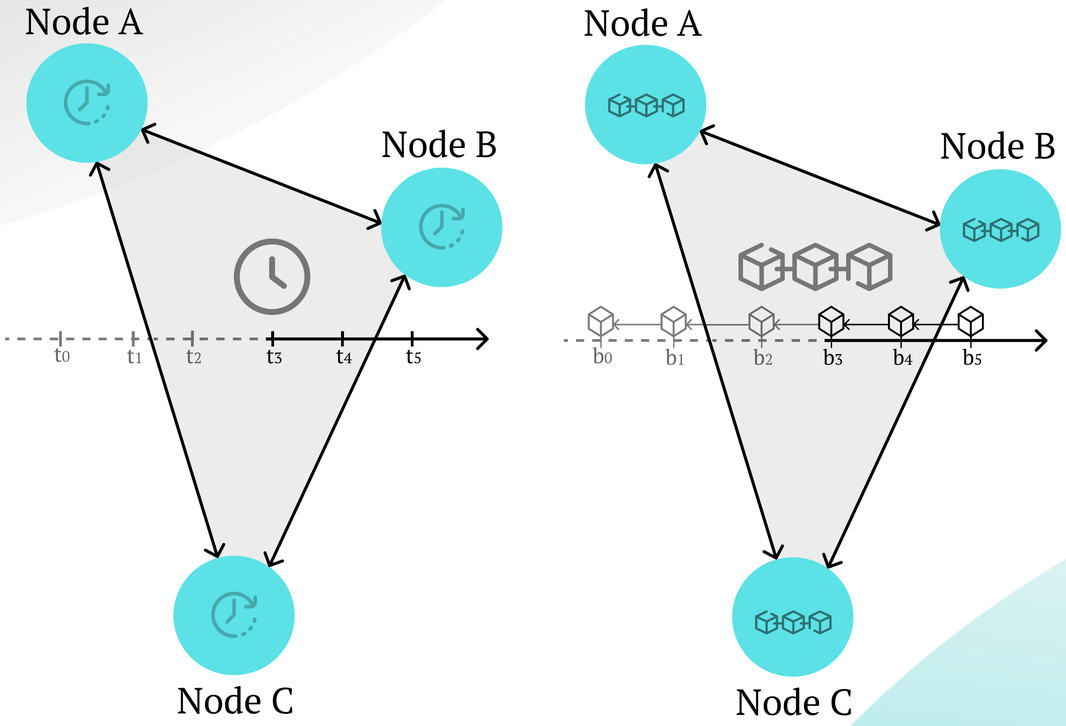


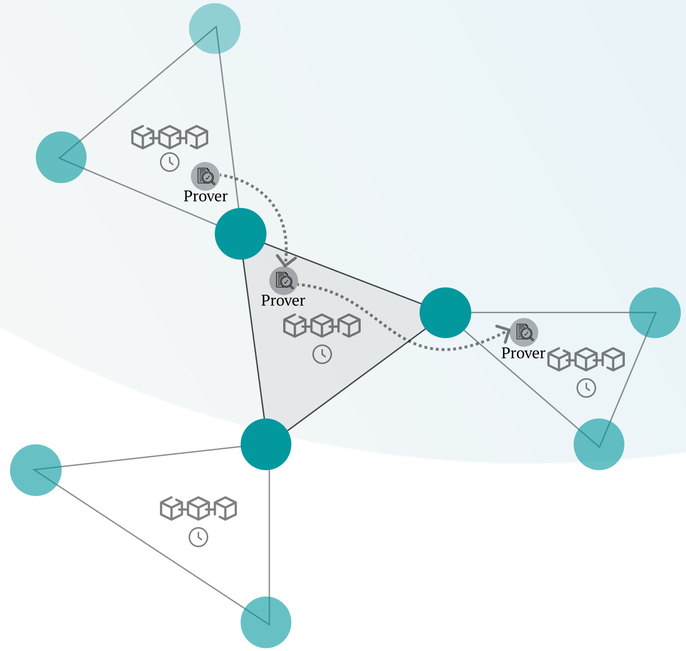


1. **Physical Layer**:
    - The bridge interface pooling all raw mesh traffic.
2. **Data link Layer**:
    - The MAC sublayer and the batman-adv protocol.
3. **Network and Transport Layers**:
    - Subnetting and the TCP/IP suite.

Turing-Complete Clock Synchronization

Permissionless Consensus Mechanisms



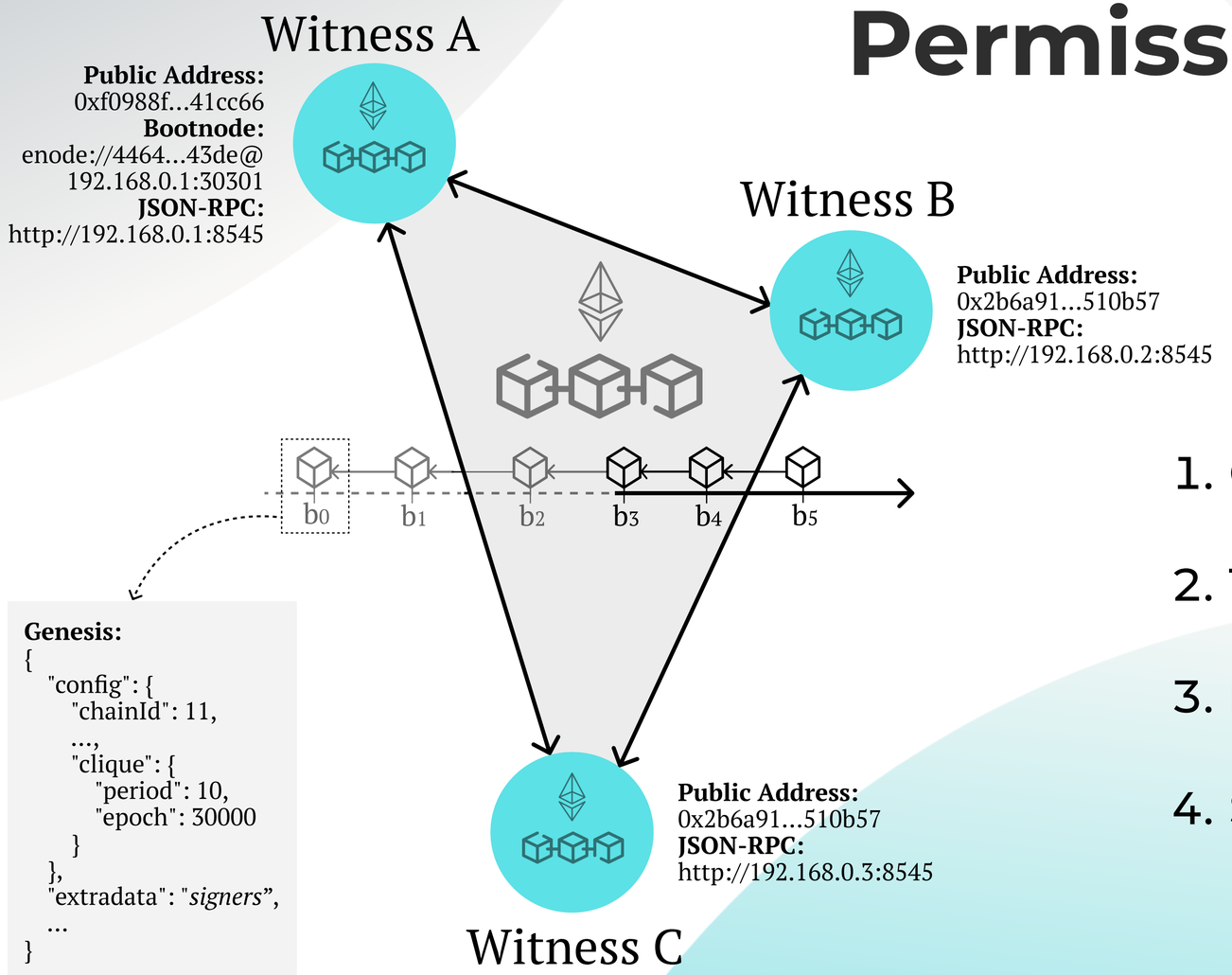


A **consensus mechanism** allows for:

- establishing zone-relative time consciousness
  - with strongly consistent serialization of transactions and
  - total order of multidimensional events.
- the decentralized execution of programs
  - via smart contracts.

Practical Permissionless Consensus

Ad-hoc Ethereum Network

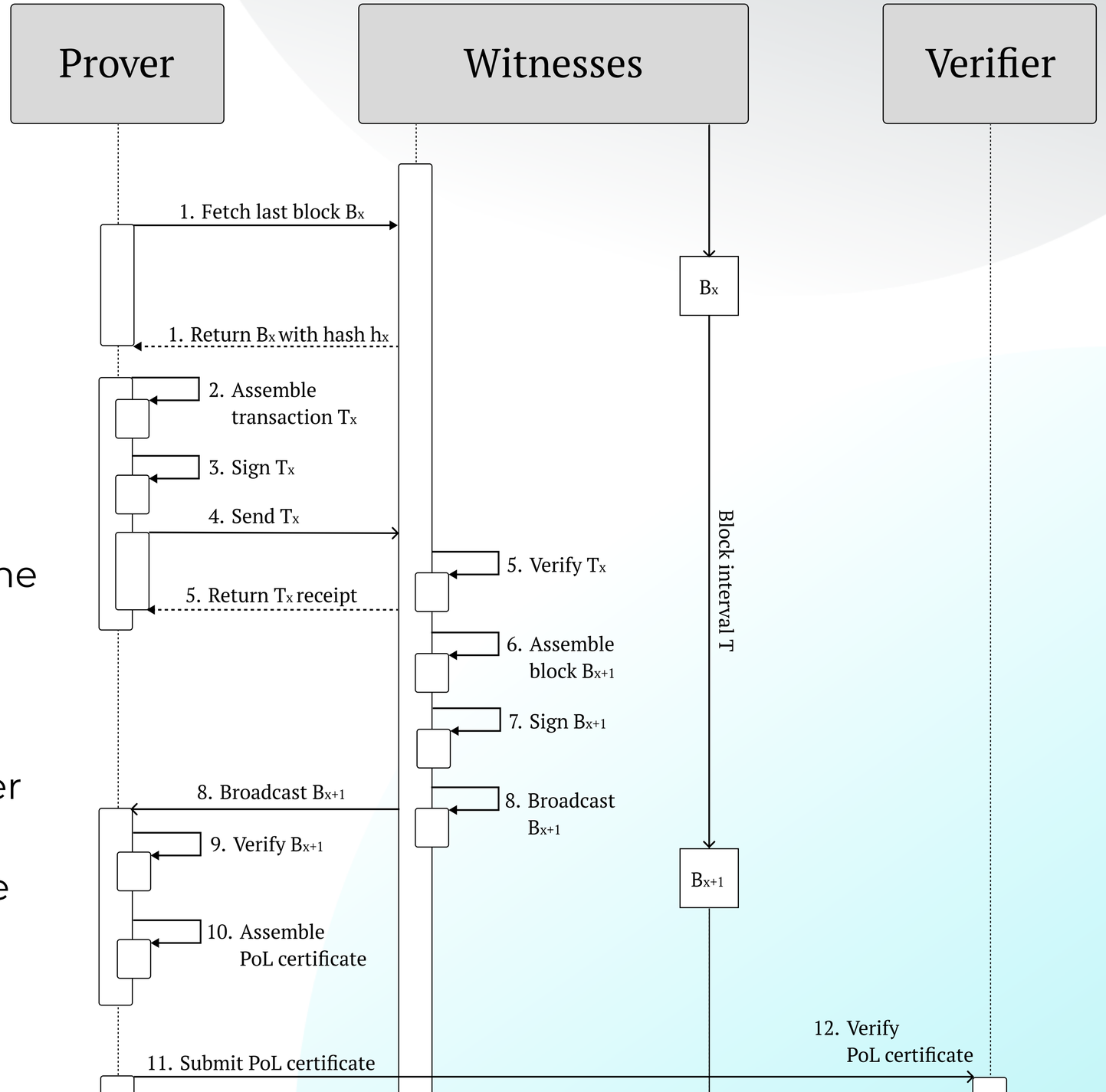


1. Consensus protocol:
   - Proof-of-Work vs Proof-of-Authority
2. The block time:
   - fixed vs dynamic
3. Initialization and discovery:
   - Genesis file and bootnodes
4. Smart contracts:
   - Solidity and EVM

Proof Generation and Verification

Prover & Verifier Processes

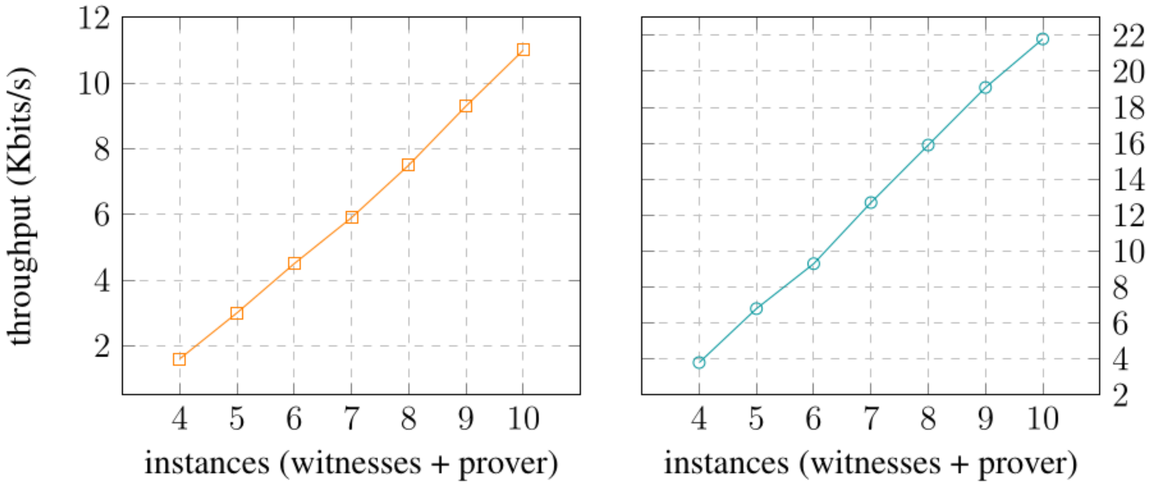
- Verifying:
  - the signatures of block B_{x+1} and transaction $T_{x\rho}$.
  - the transaction input matches the parent hash h_x of the block.
- Ensuring:
  - spatial synchronization.
  - temporal alignment of the prover with zone-relative time t_{x+1}.
  - authenticity of the block and the transaction.



Measurements and Attack Vectors

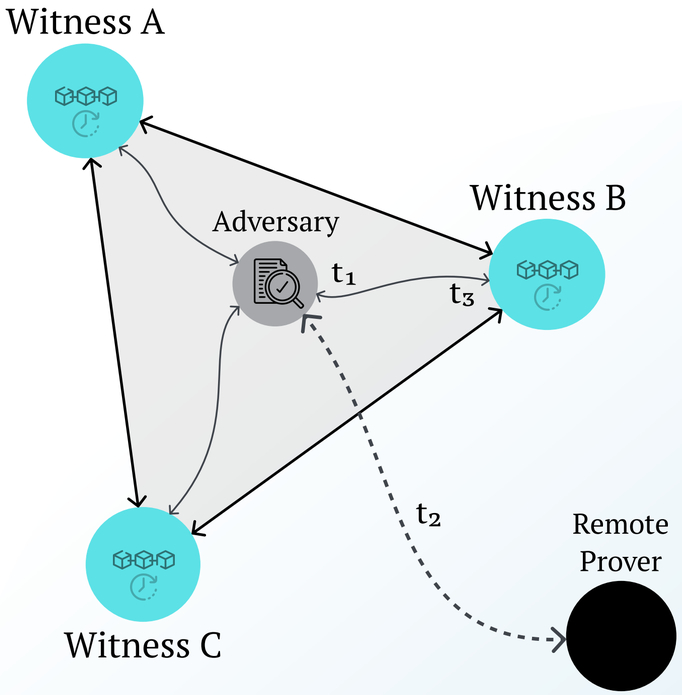
Block time and Proxy attacks

1. Average protocol throughput:
   - linear increase with the increase in the number of witnesses.
   - peaks of TCP traffic during the block proposal phase.
2. Low CPU, RAM and Disk usages:
   - suitable for resource-constrained environments.
3. Success rate:
   - directly dependent on the block time.
   - possibility for proxy attacks.



(a) Batman-adv traffic throughput.

(b) IPv4 traffic throughput.

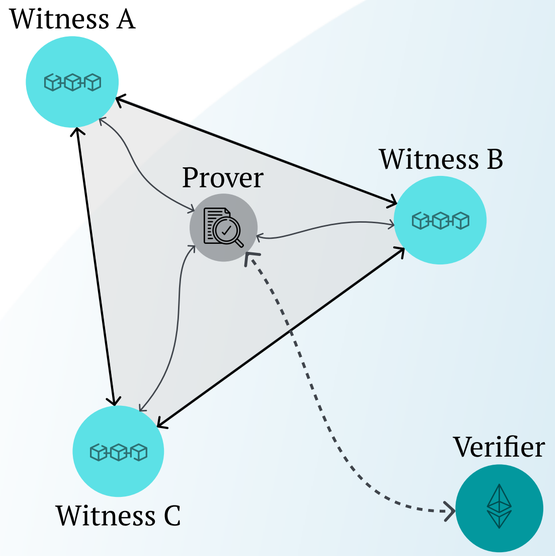


16th May 2023 — Distributed Systems Seminar

Towards Decentralized Proof-of-Location

In this thesis, we:

- Dissected the Proof-of-Location paradigm.
- Reviewed the state of the art.
- Specified a novel decentralized protocol.
- Implemented a proof-of-concept.



Eduardo Ribas Brito
Supervised by Ulrich Norbisrath

UNIVERSITY OF TARTU
Institute of Computer Science
1632

Appendix

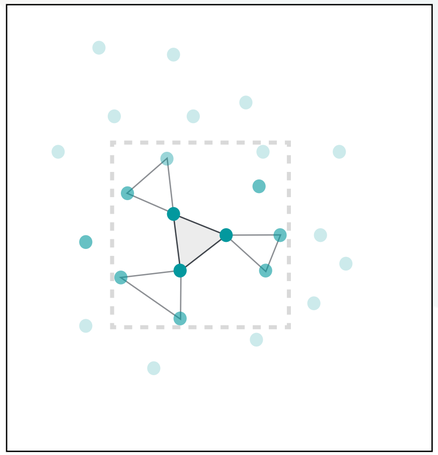
Overview

Protocol Fundamentals

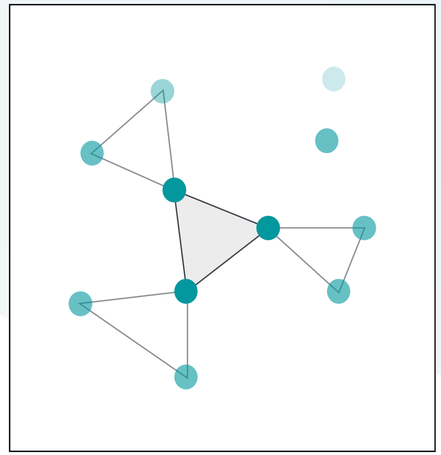
From a dynamic mesh topology, towards the ultimate goal of achieving Absolute Proof-of-Location.

A. Mesh Network

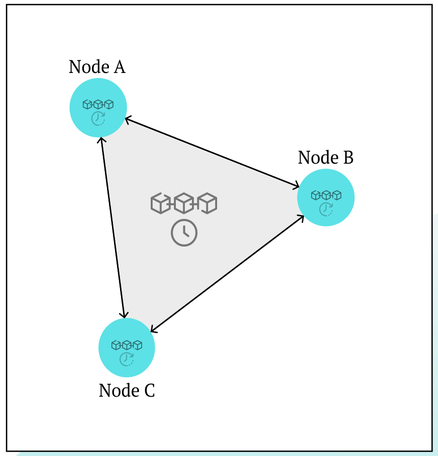
B. Zone Discovery



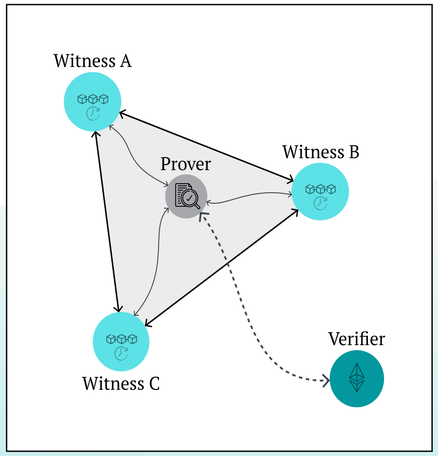
C. Zone Affinity



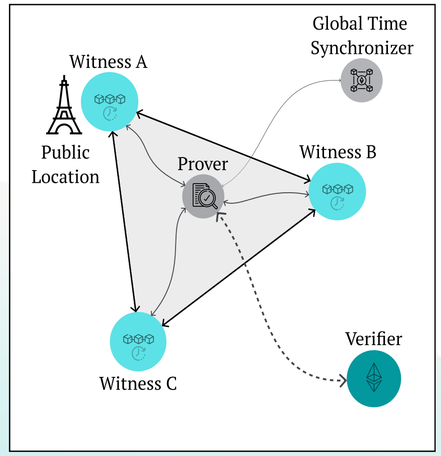
D. Zone Synchronization



E. Relative Proof-of-Location



F. Absolute Proof-of-Location

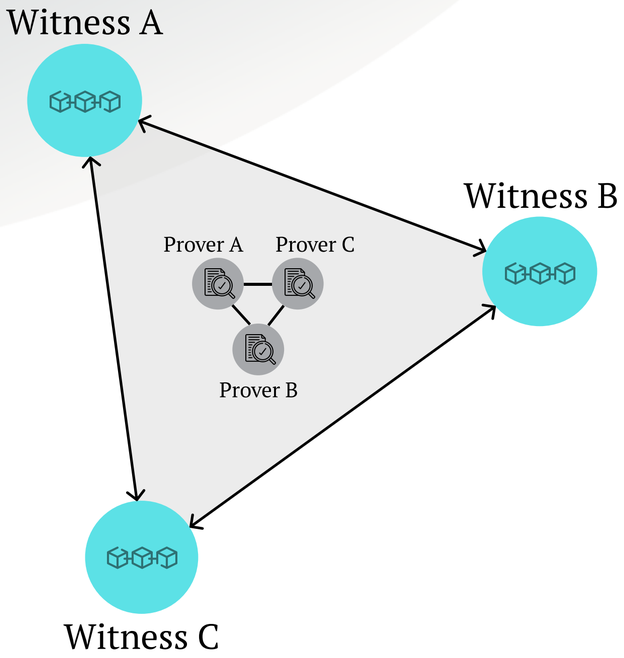


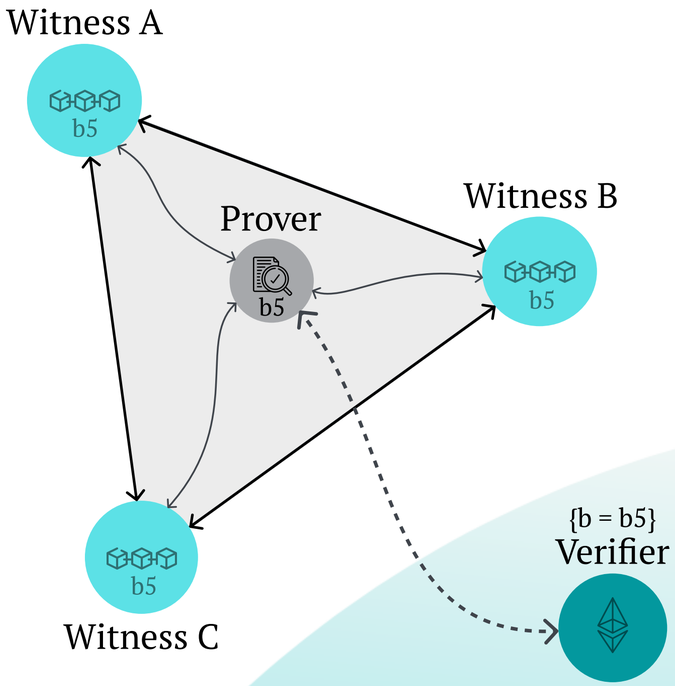
short-range, synchronous communication

long-range, asynchronous communication

Smart Contracts

Turing-Completeness use cases



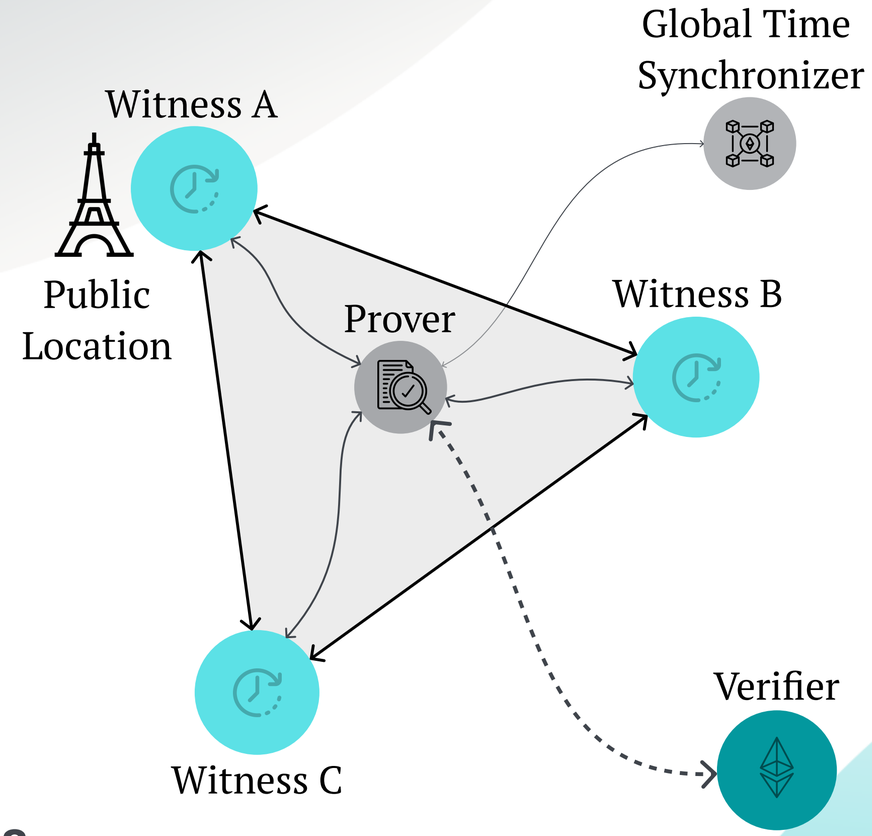


A Turing Complete Proof-of-Location protocol enables:

- On the left,
  - a multi-prover configuration, attesting the simultaneous existence of a group of provers
- On the right,
  - a verifier enforcing the attestation of the prover's location at a specific block or time.

Absolute Proof-of-Location

From Relative Proof-of-Location



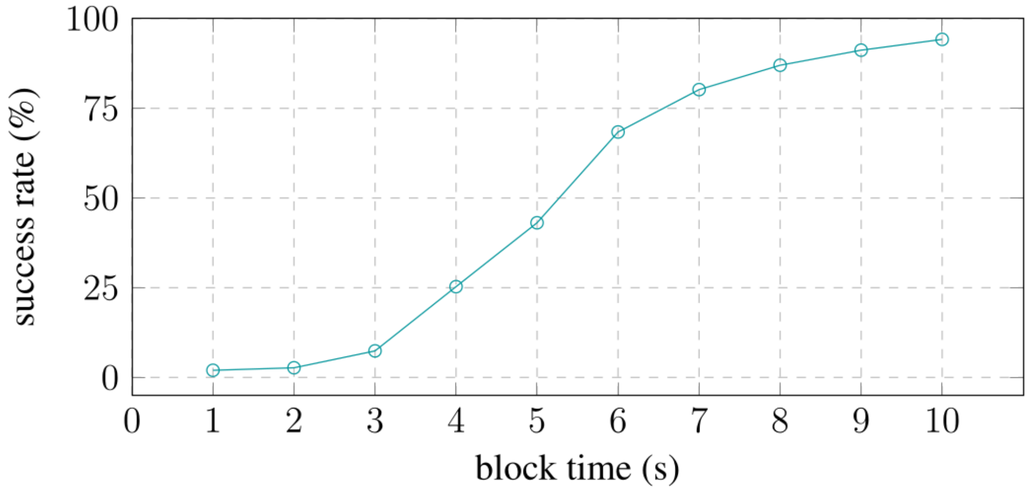
A Proof-of-Location certificate to be spatially and temporally acknowledged by any other node outside the zone needs:

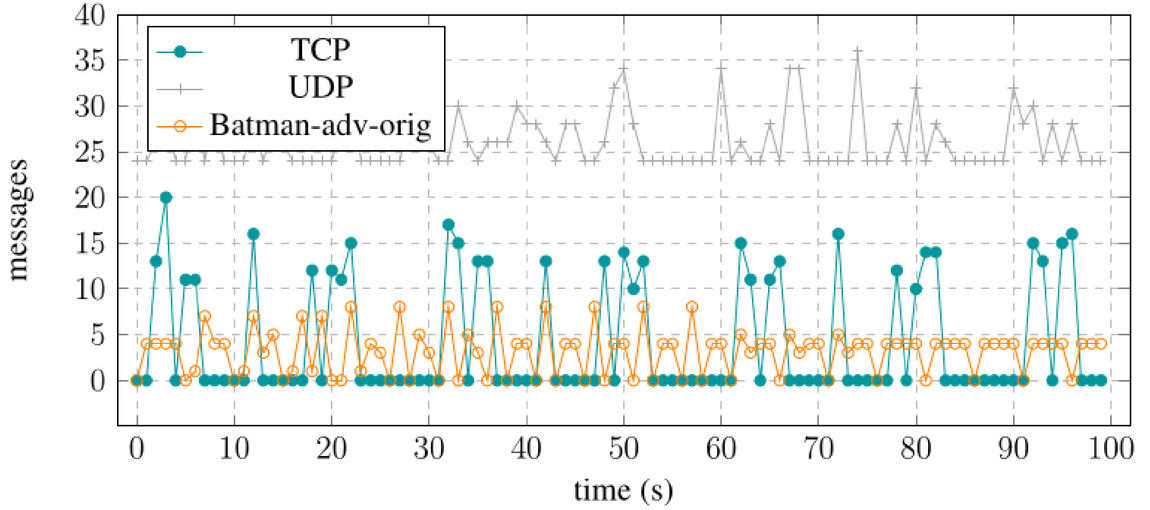
- Global Time Synchronization Protocol
  - NTP, PTP, Public Blockchain?
  - Trusted timestamping?
- Global Positioning System
  - GPS, crypto-spatial coordinates?

Measurements

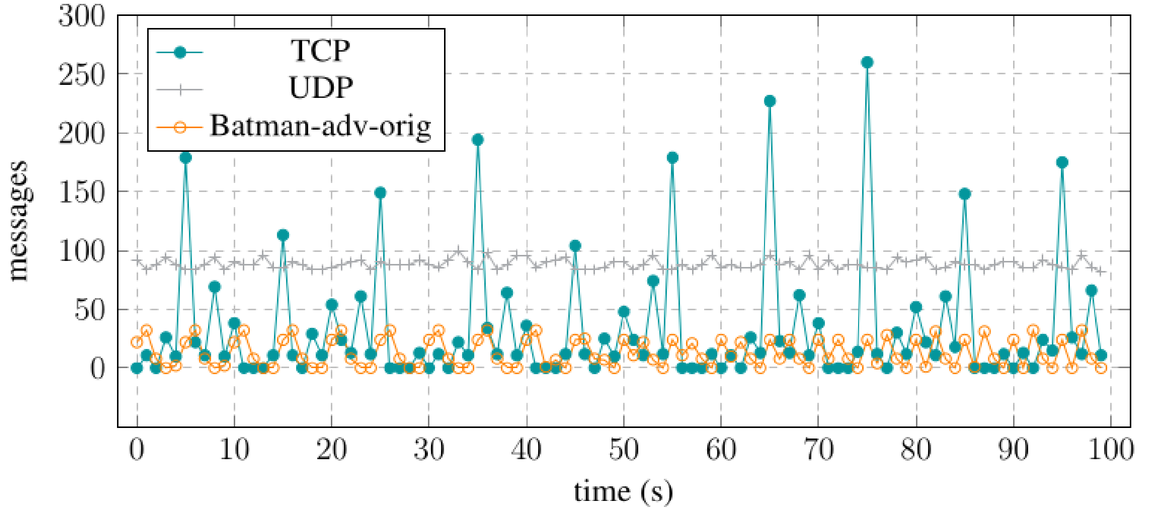
Blockchain Activity & Success Rate

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.

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