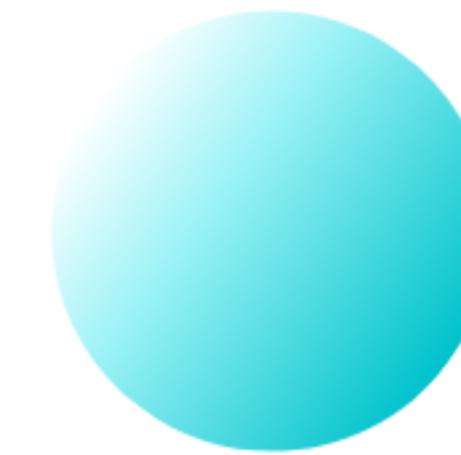


20th of May 2023

Distributed Systems Seminar

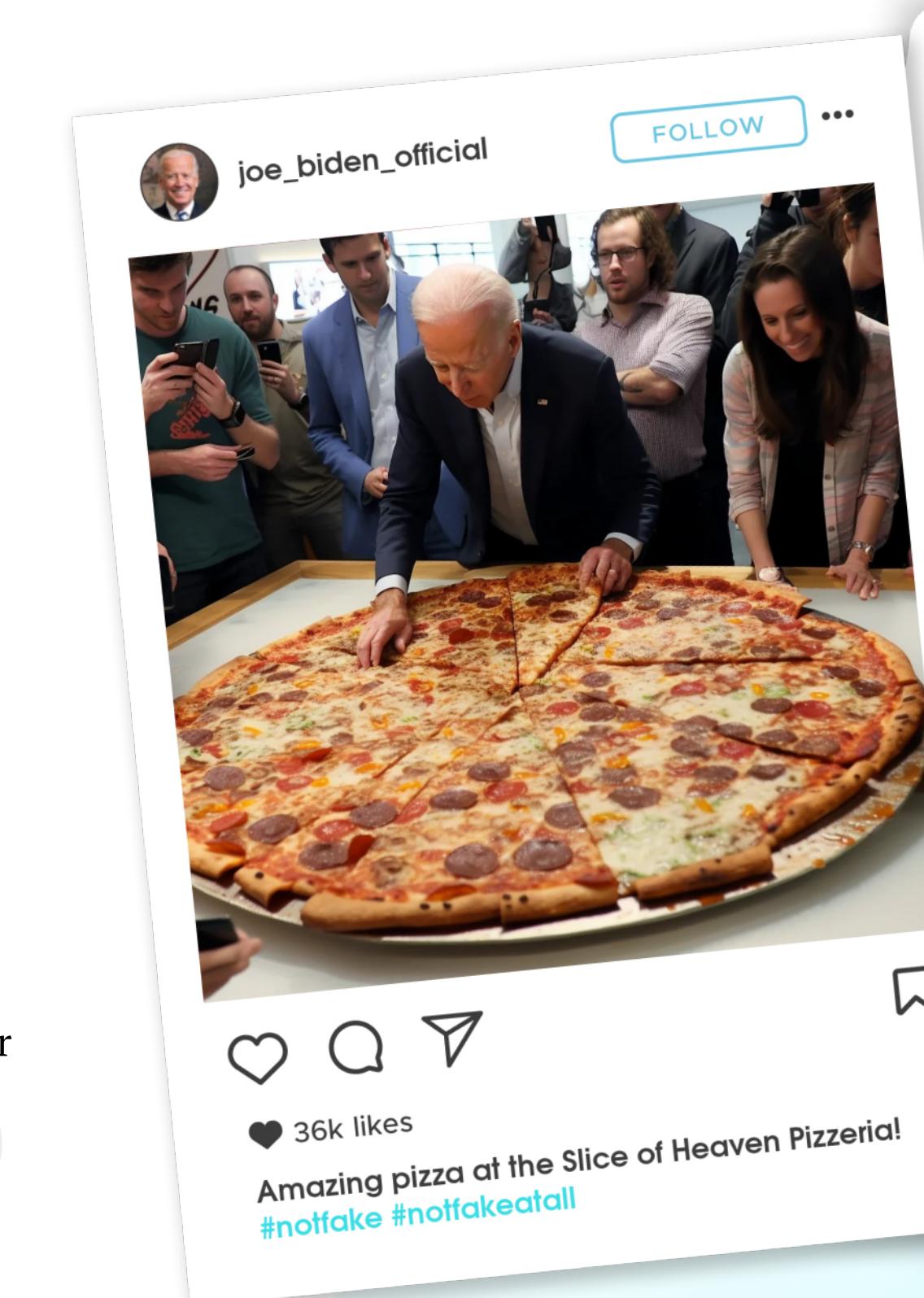
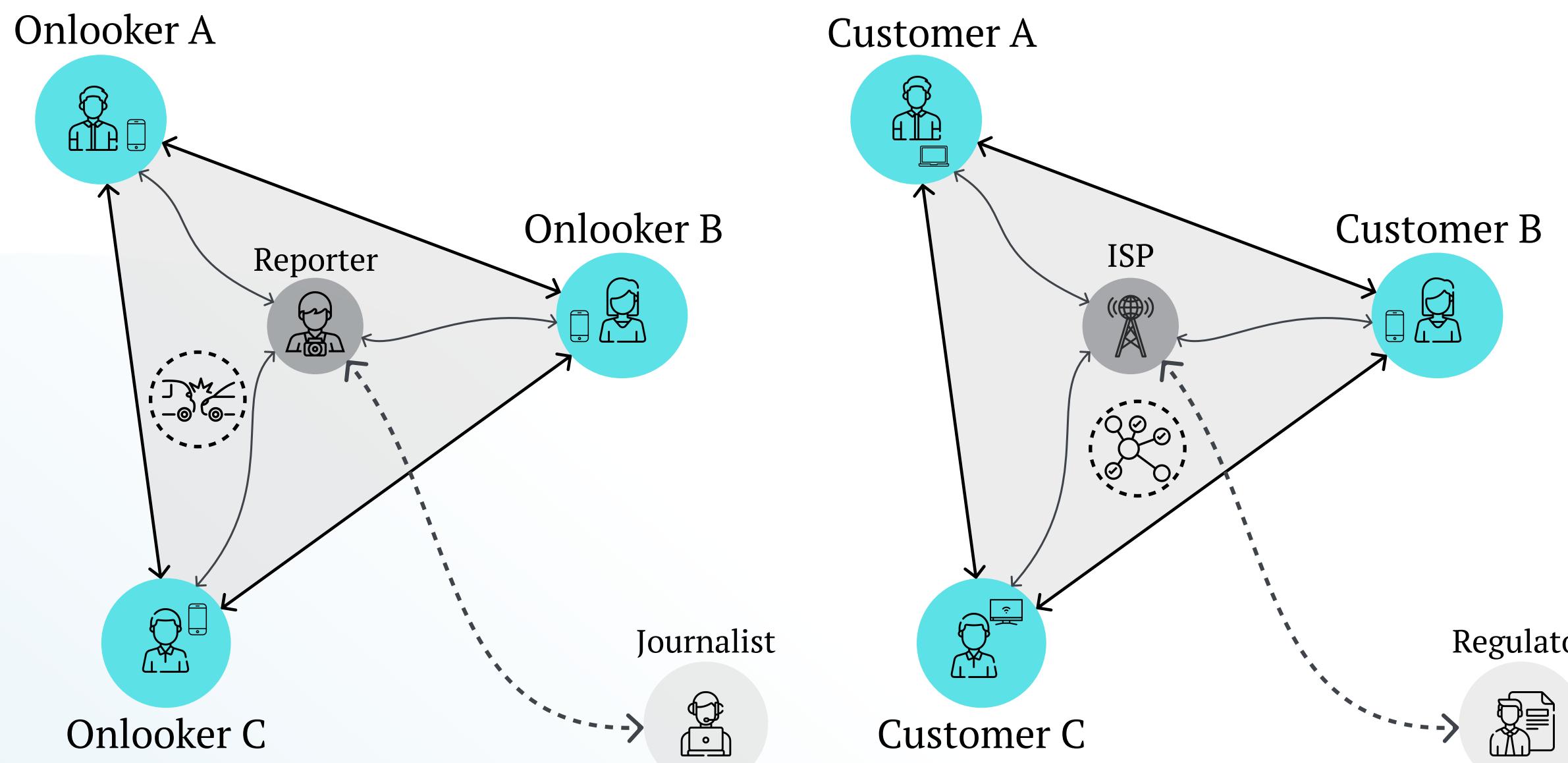
Towards Decentralized Proof-of-Location



Eduardo Ribas Brito
Supervised by Ulrich Norbisrath

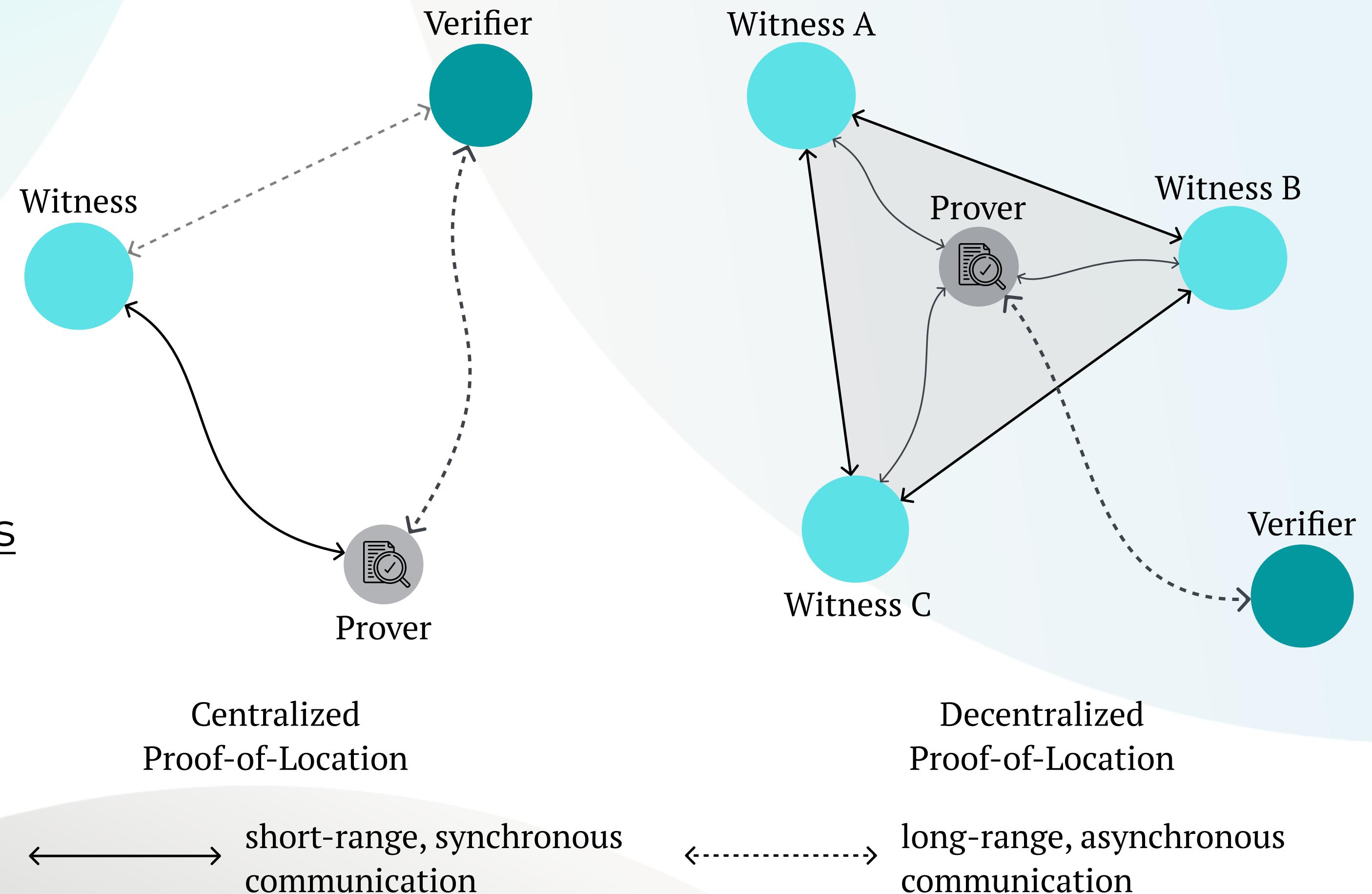
UNIVERSITY OF TARTU
Institute of Computer Science

Location-based Authentication/Authorization In Adversarial Environments

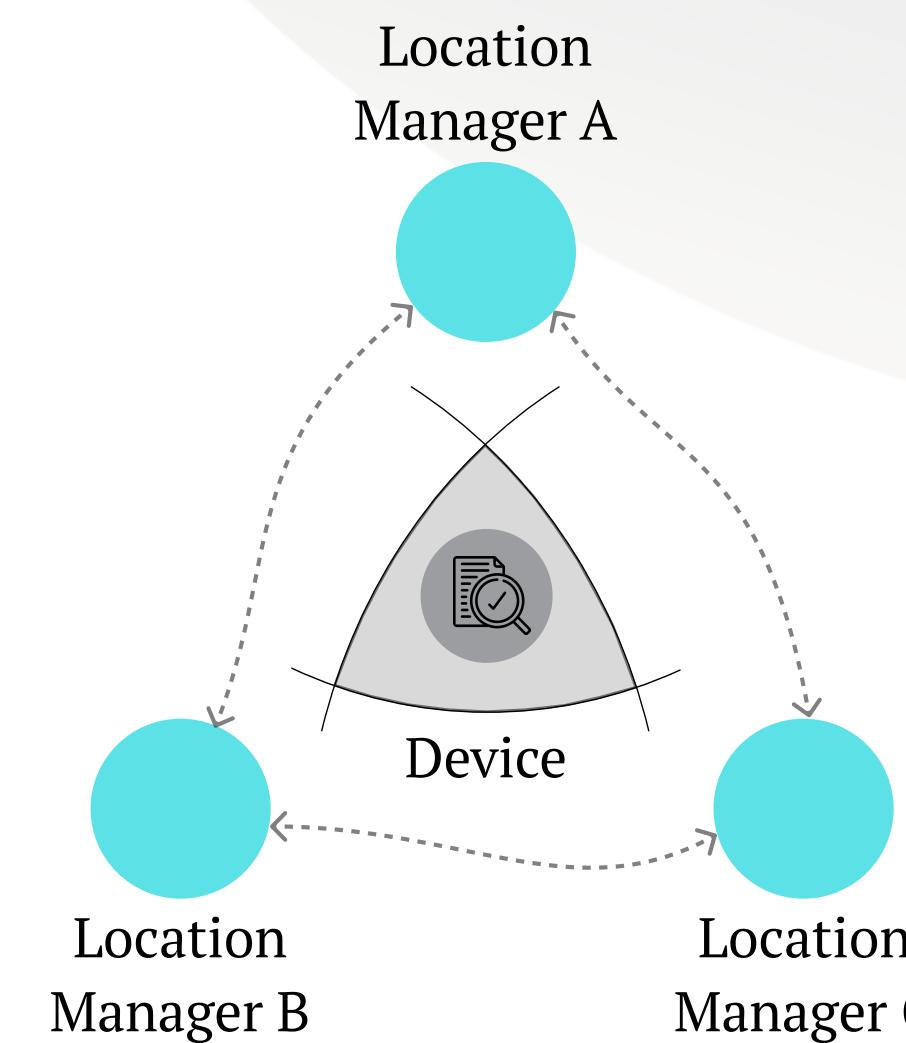
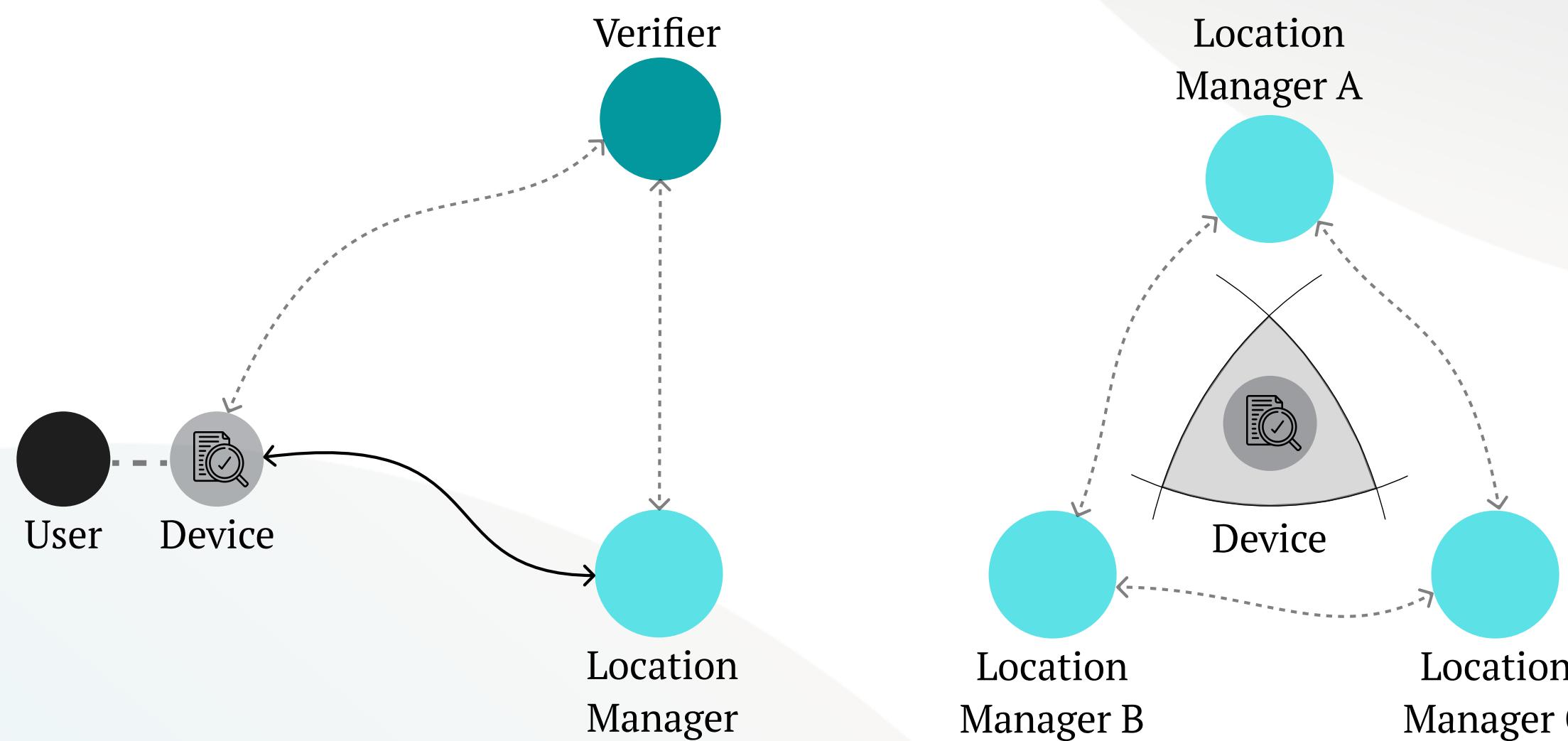


A digital Proof-of-Location

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

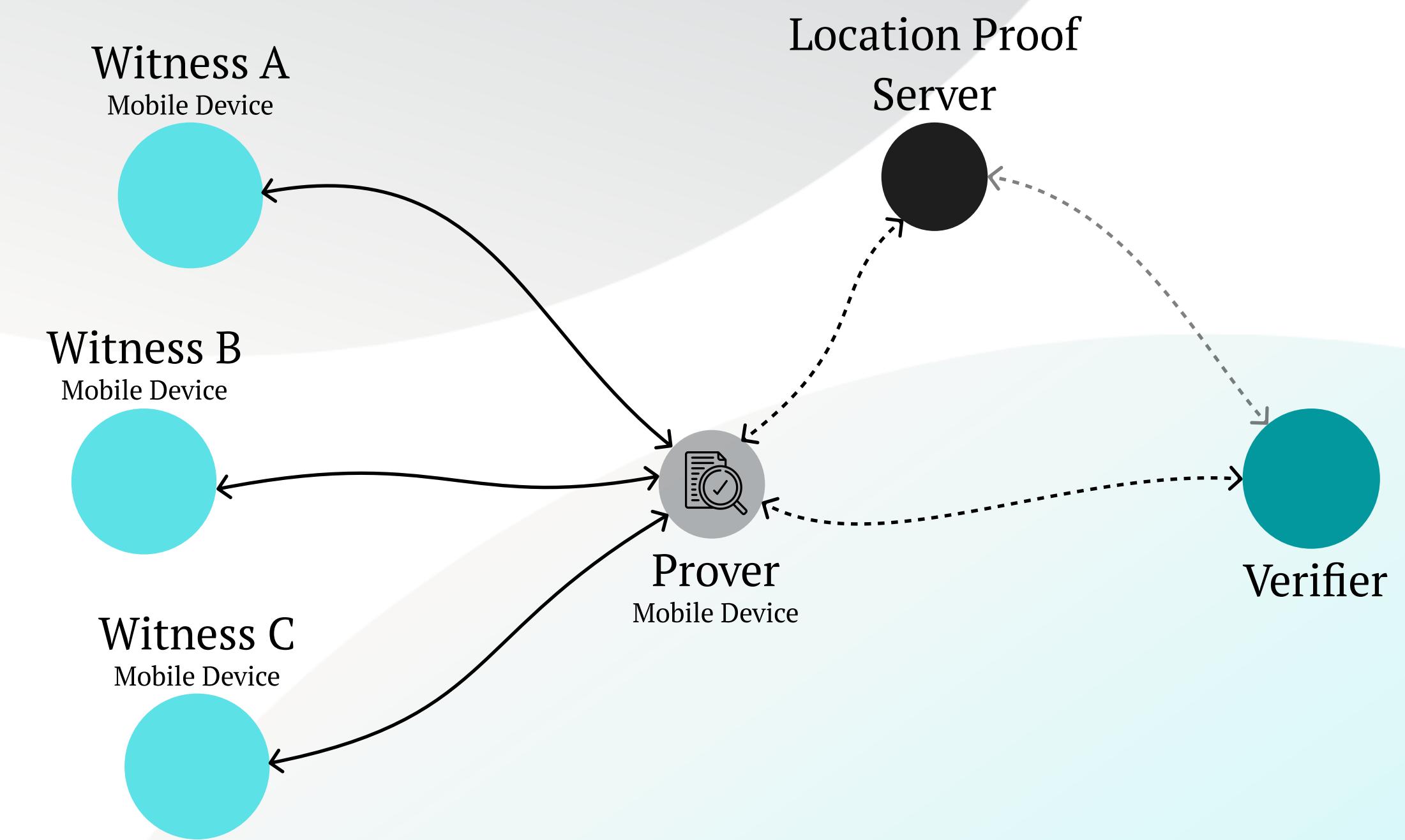


The evolution of Location Proof Systems



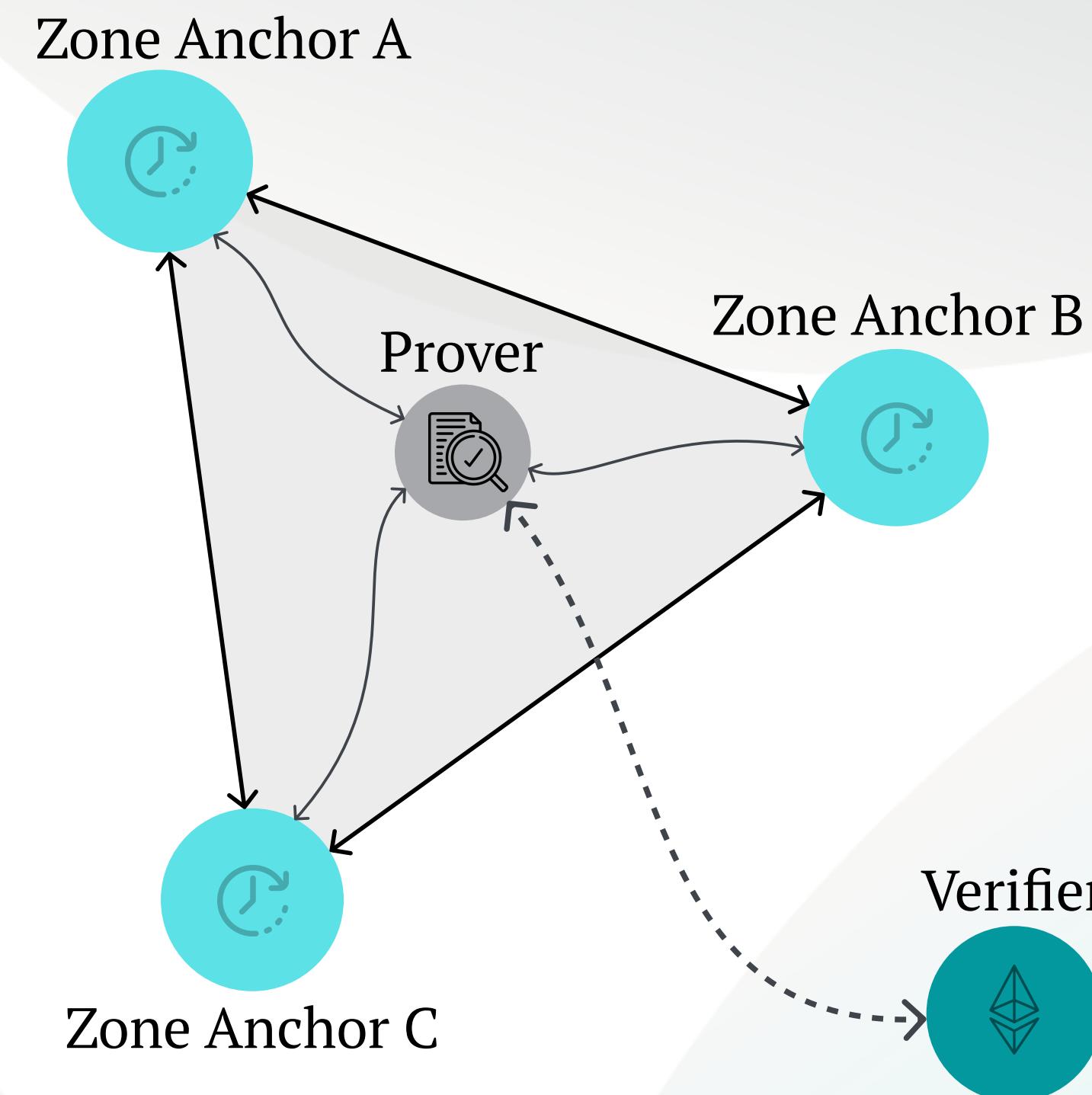
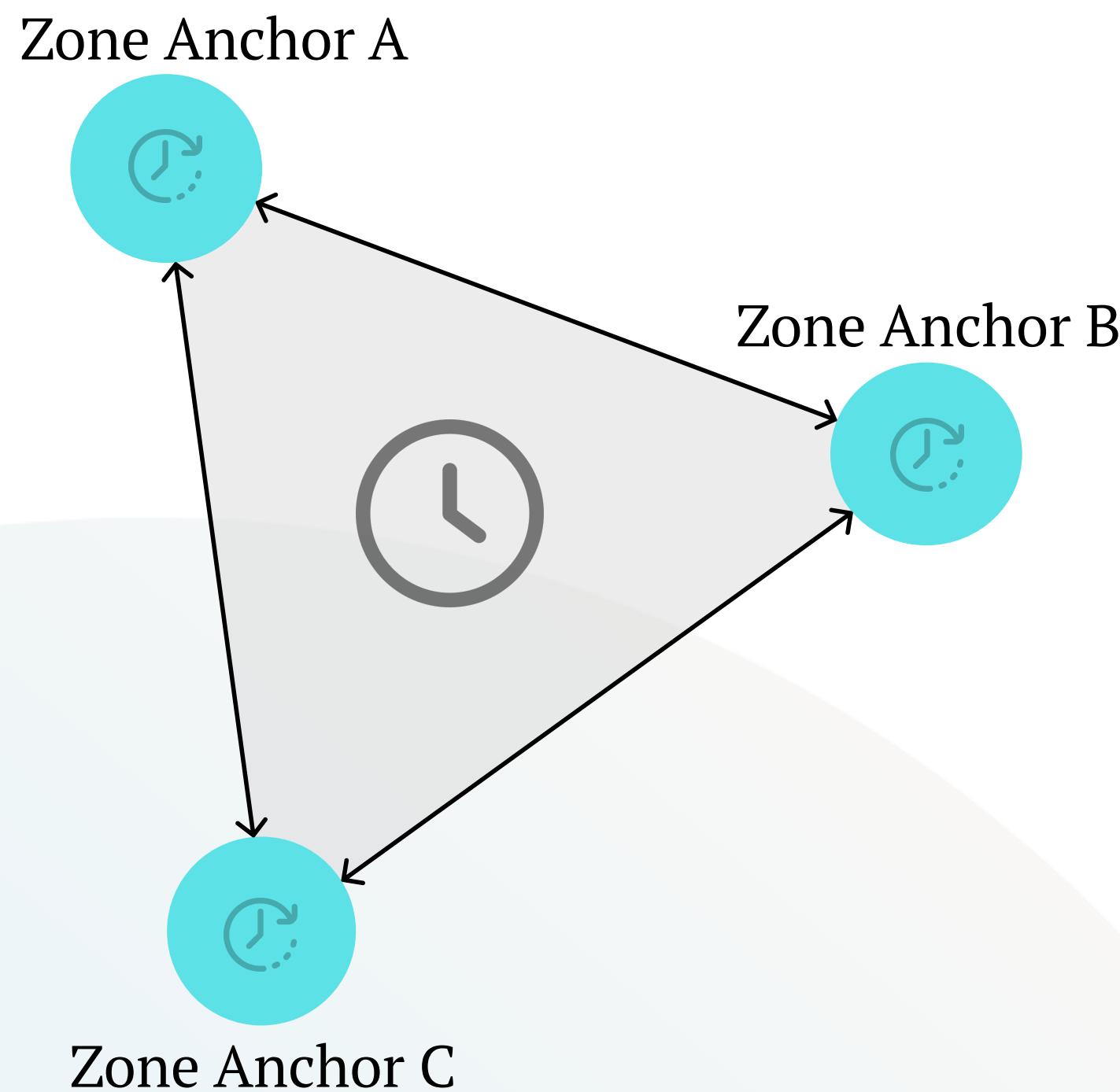
Trusted and
Centralized Architectures

04



Progressively Distributed
Systems

The evolution of Location Proof Systems

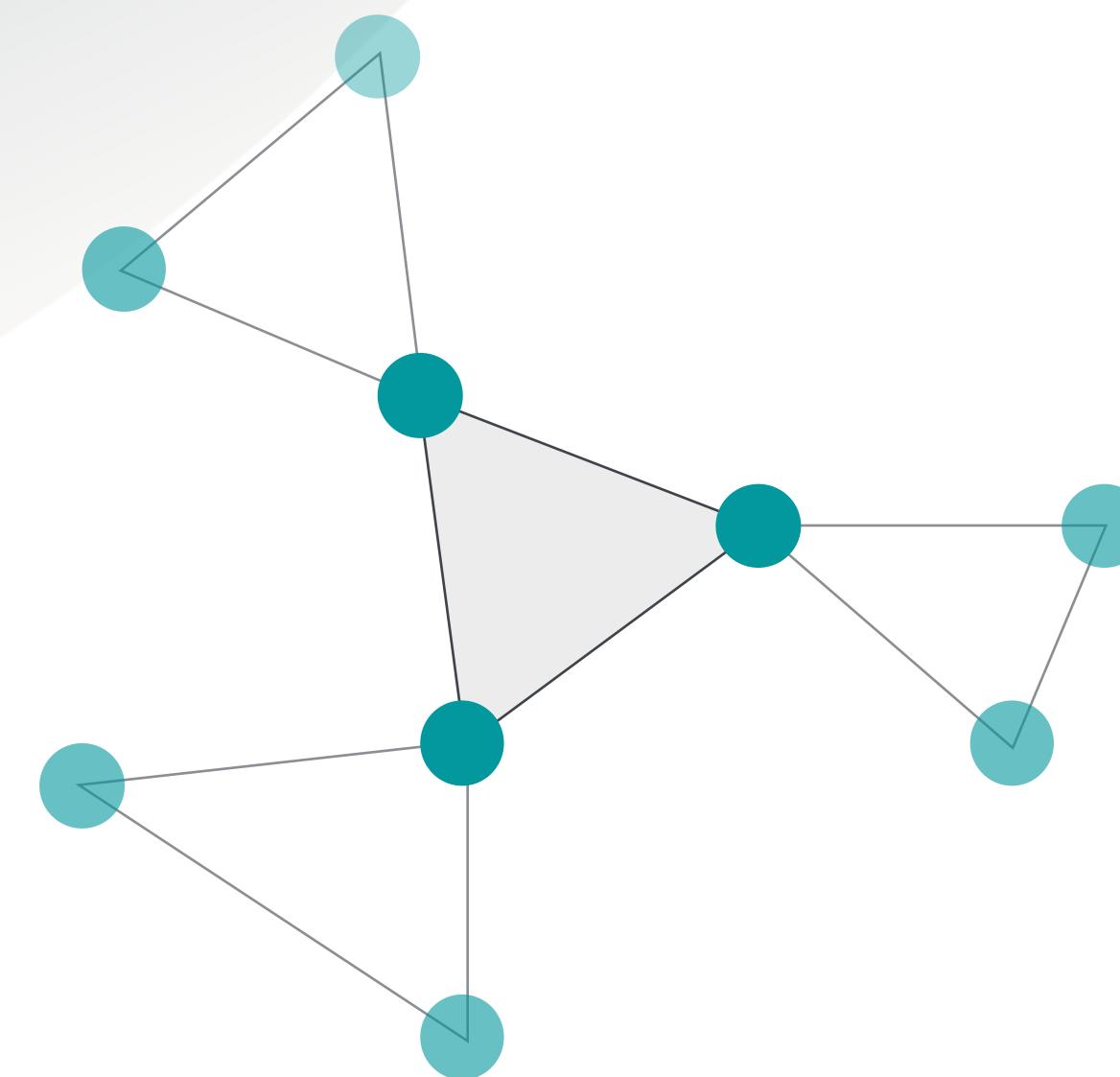


Considered secure if:

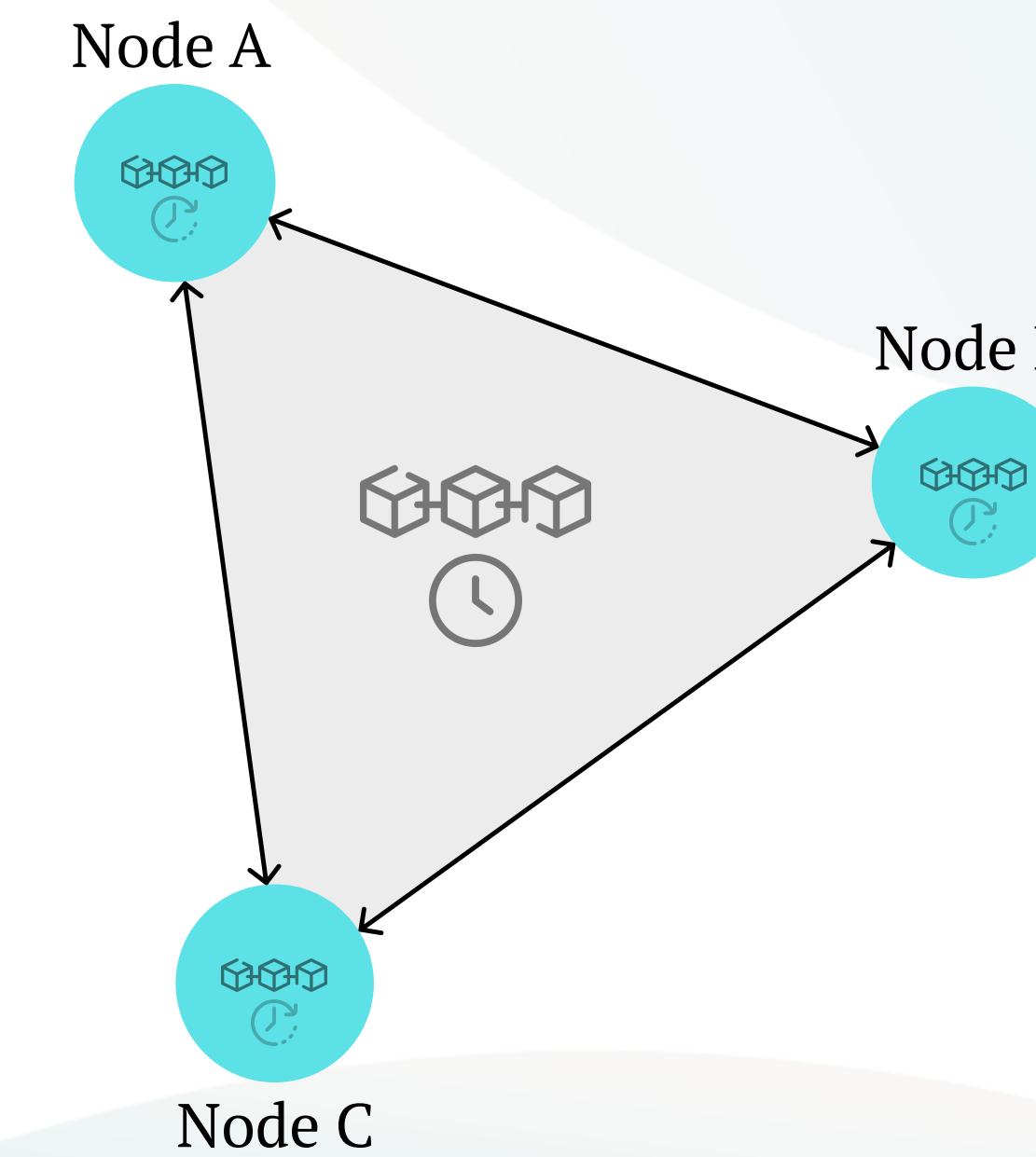
- Complete
- Spatio-temporally sound
- Non-transferable

Decentralized and Trustless
Protocols

Space Synchronization + Time Synchronization



=

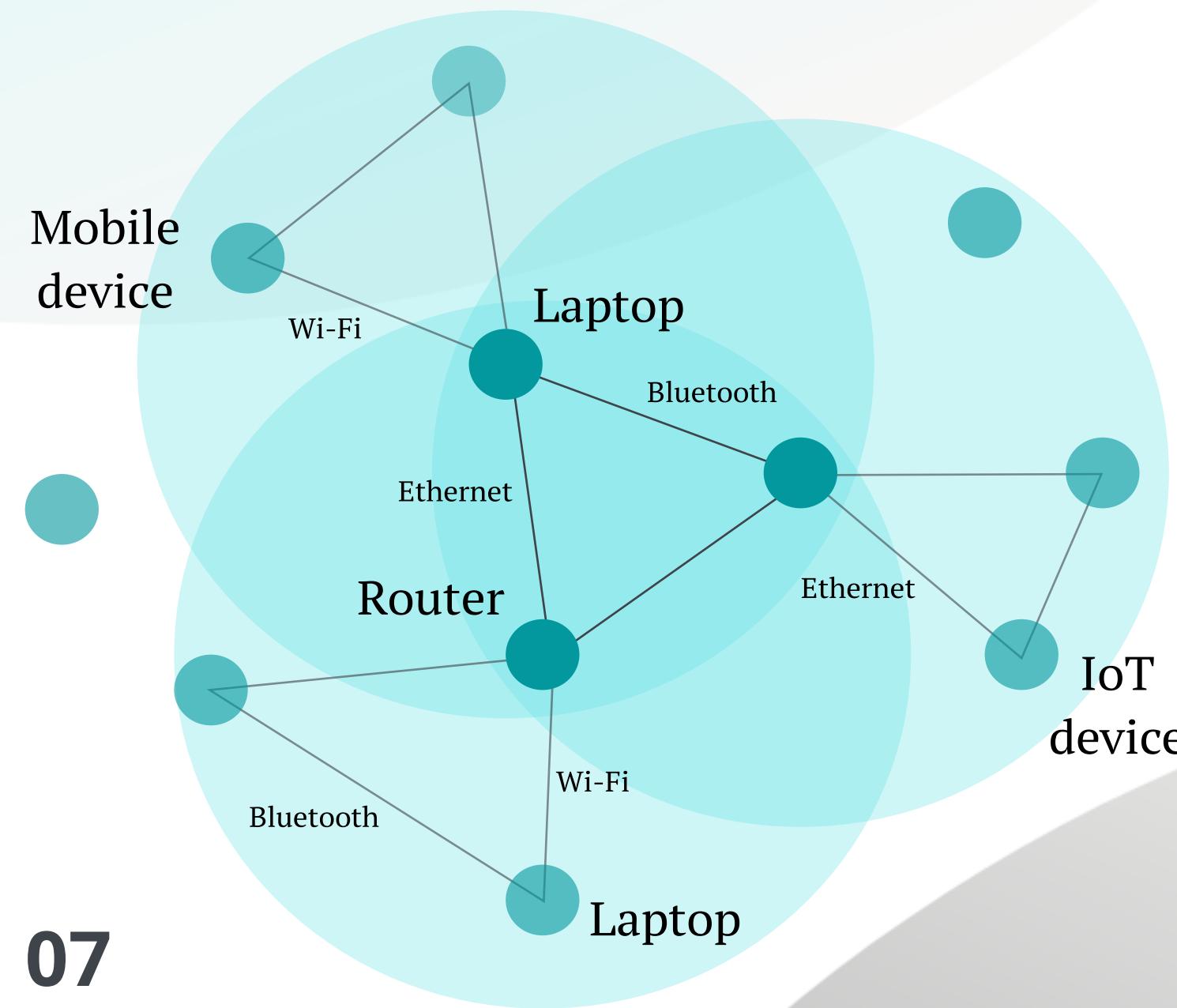


**Trustless
Proof-of-Location**

Dynamic and Non-Hierarchic Mesh Networks

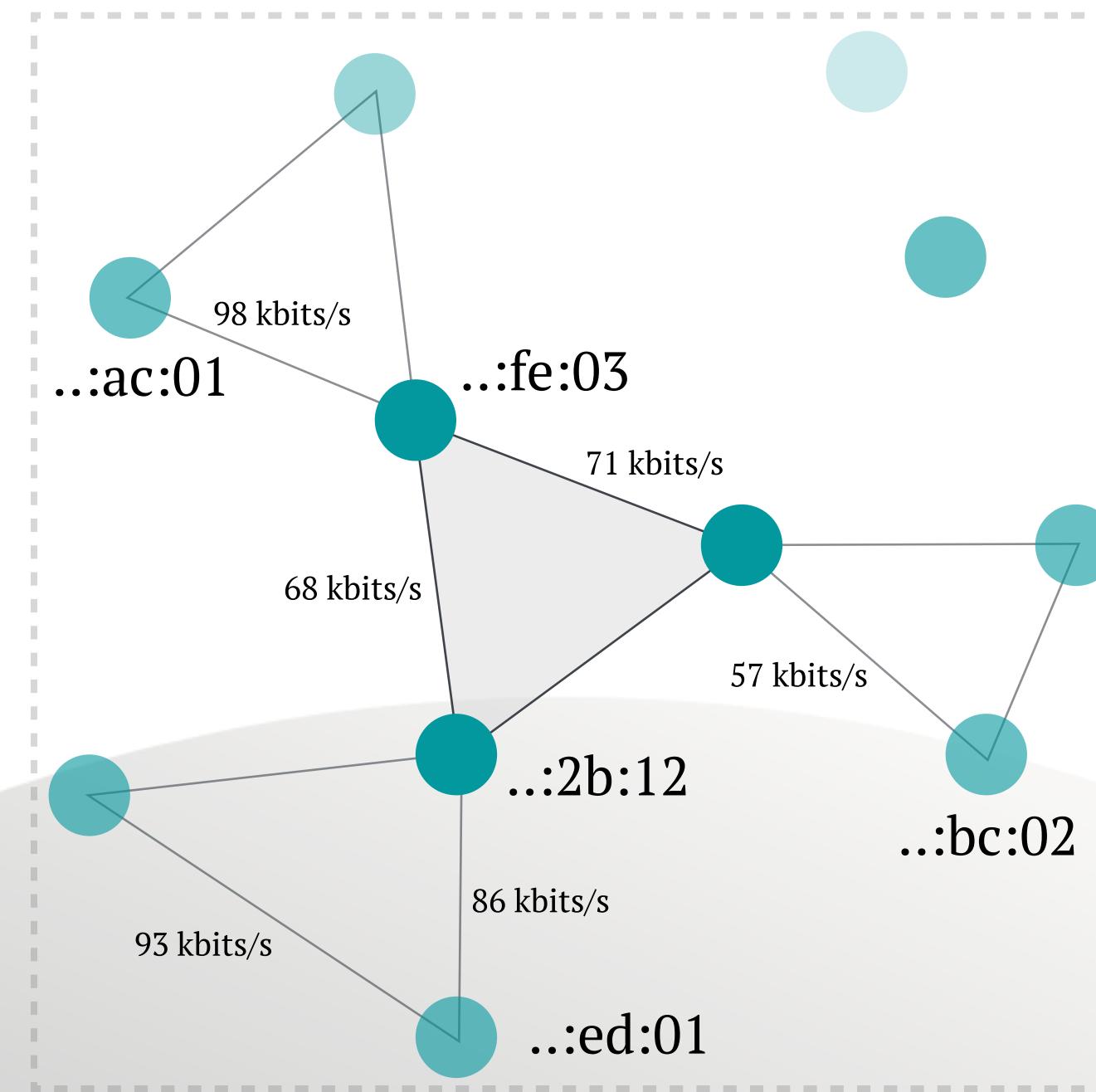
Layer 2 Routing Protocols

Peer-to-Peer
Short-ranged Communication

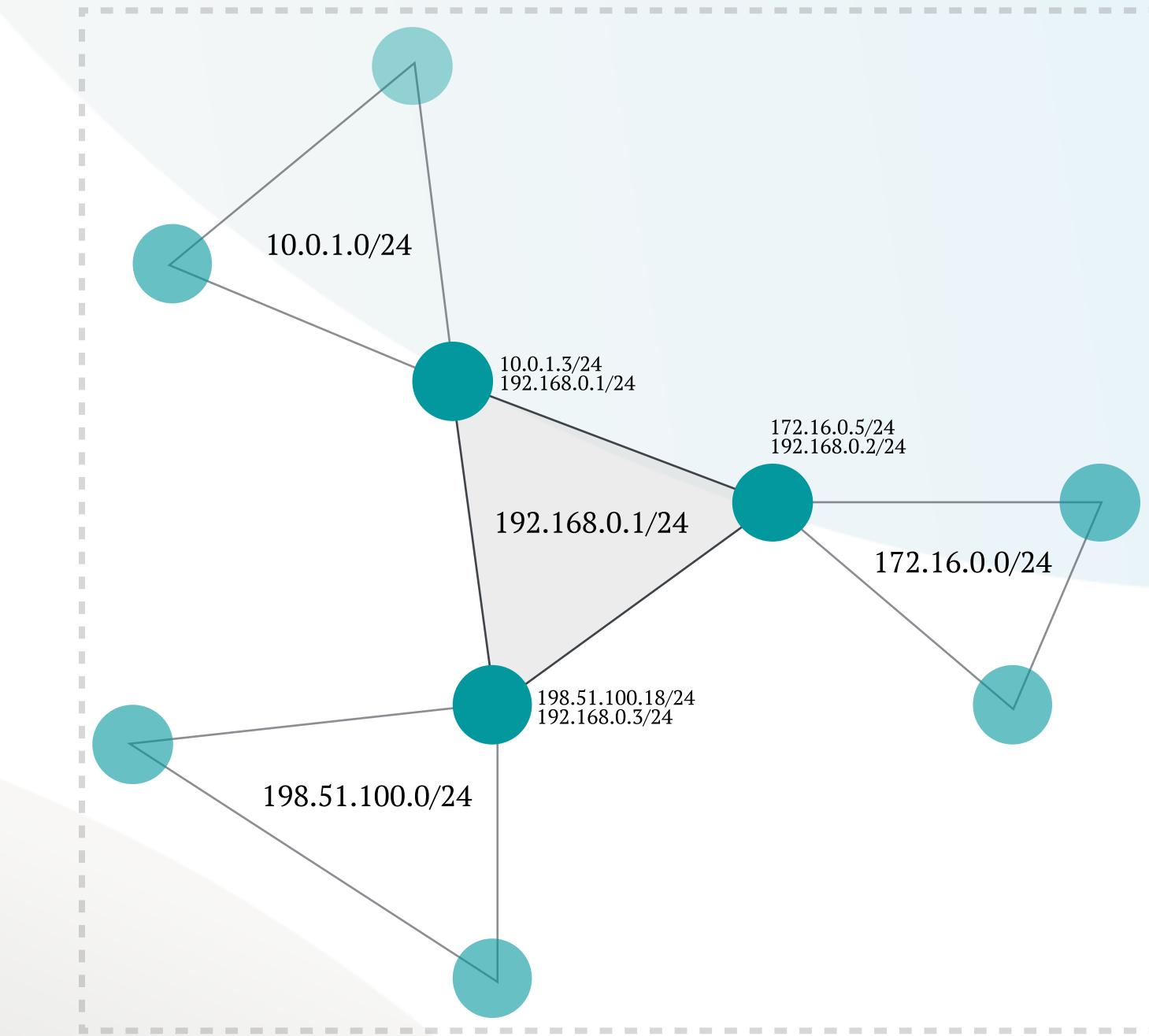


07

Neighbourhood
Discovery and Ranking

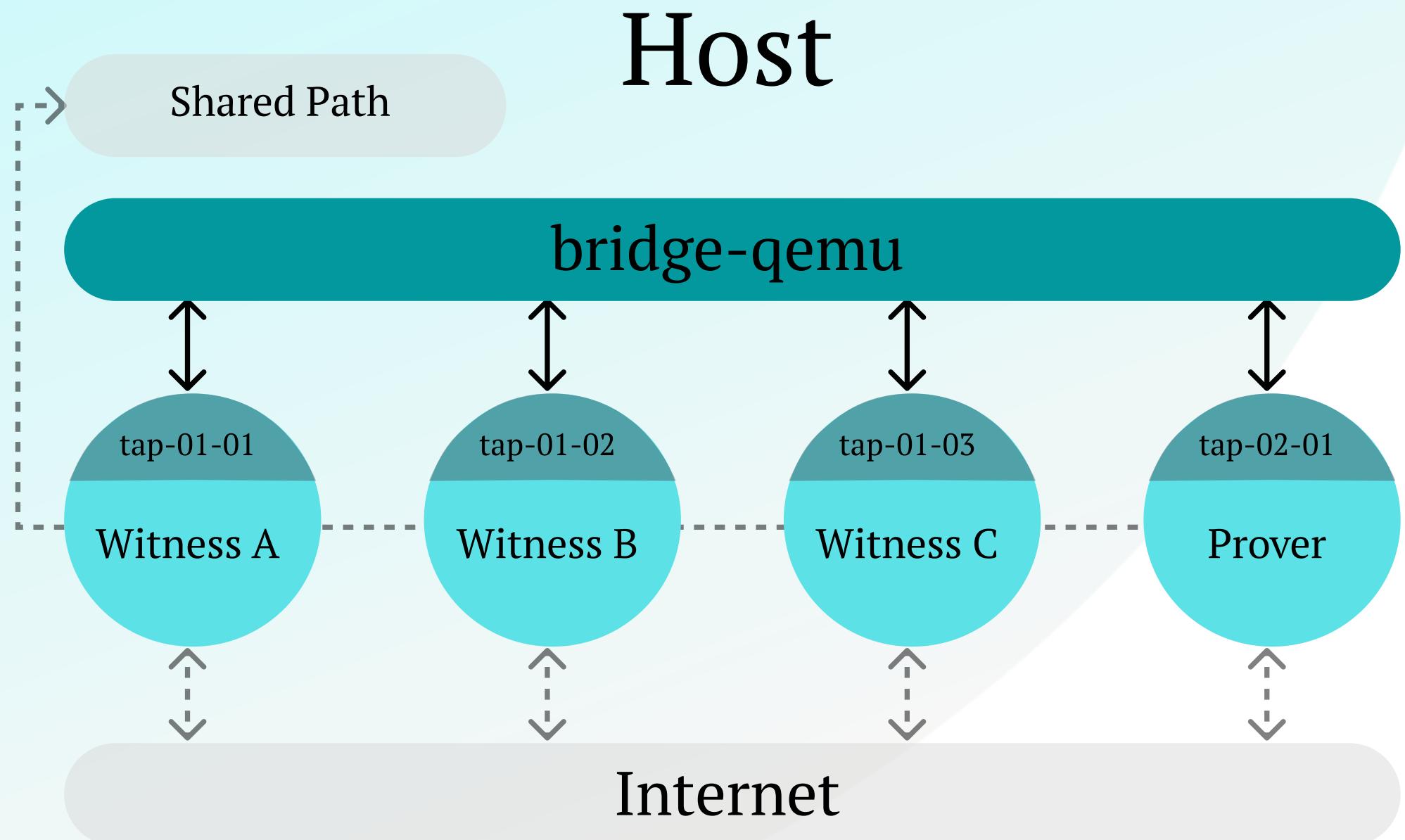


Zone Establishment
and Affinity

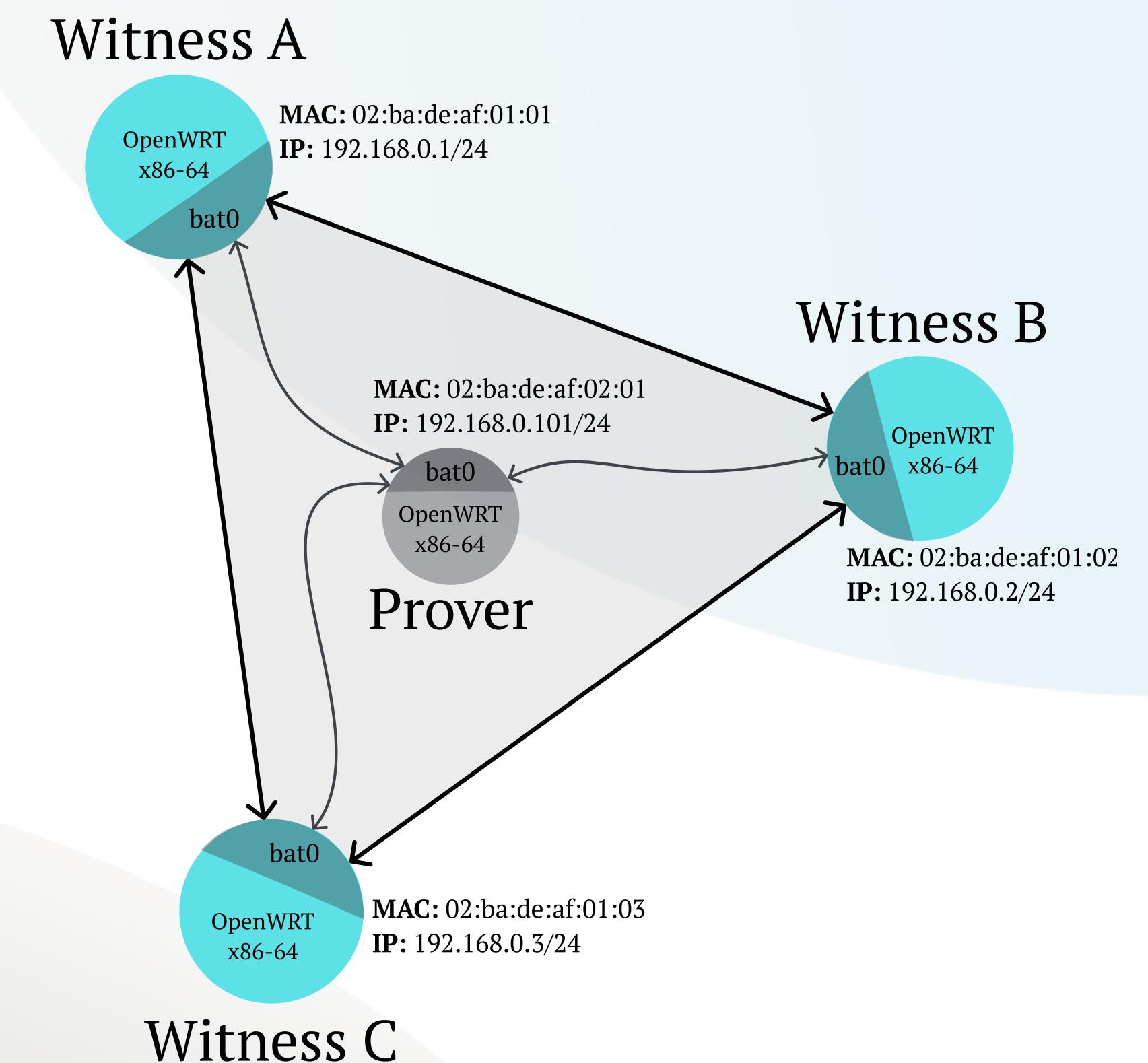


Testbed Setup and Network Architecture

OpenWRT, QEMU, batman-adv

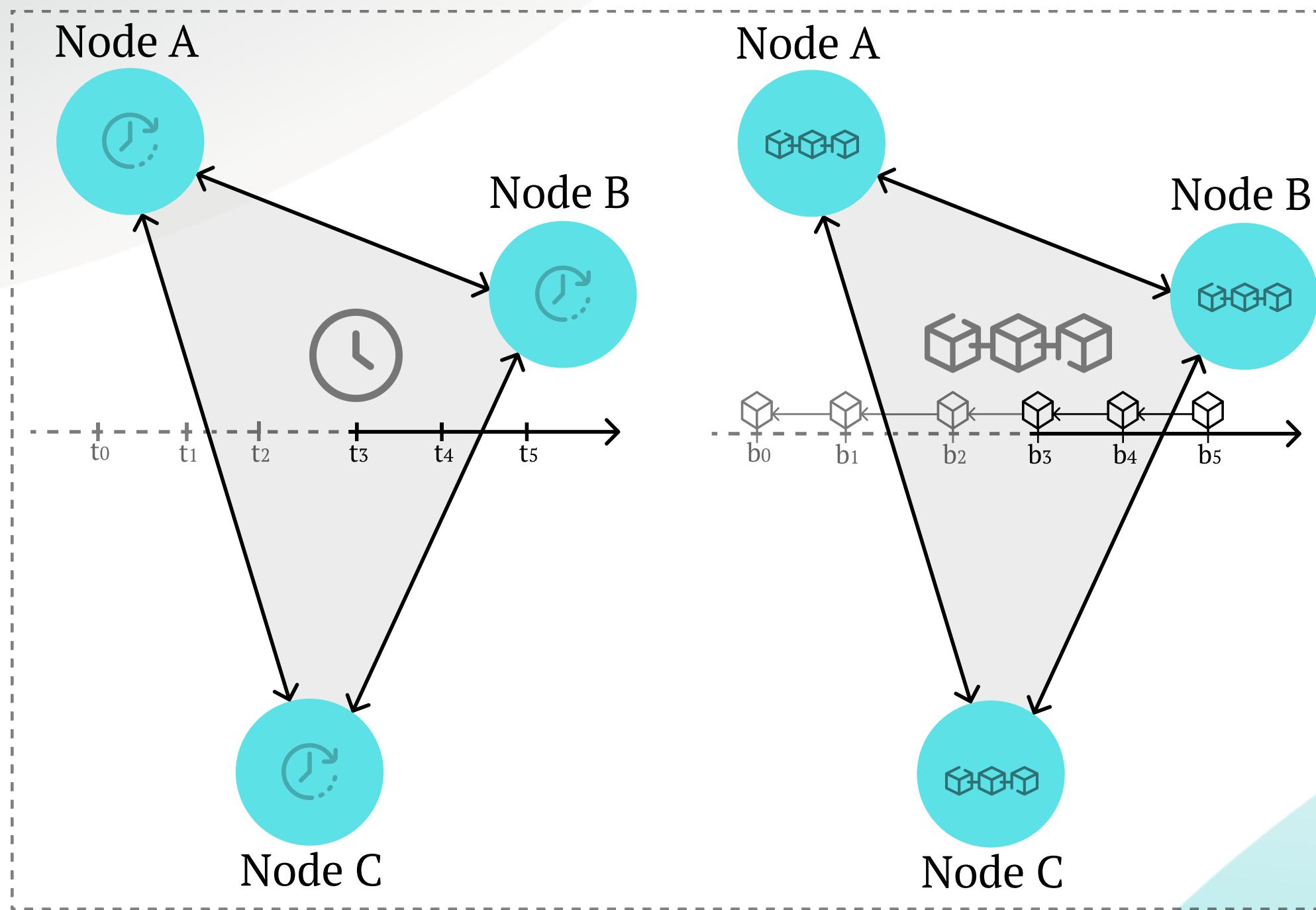


- 1. Physical Layer:**
 - The bridge interface pooling all raw mesh traffic.
- 2. Data link Layer:**
 - The MAC sublayer and the batman-adv protocol.
- 3. Network and Transport Layers:**
 - Subnetting and the TCP/IP suite.

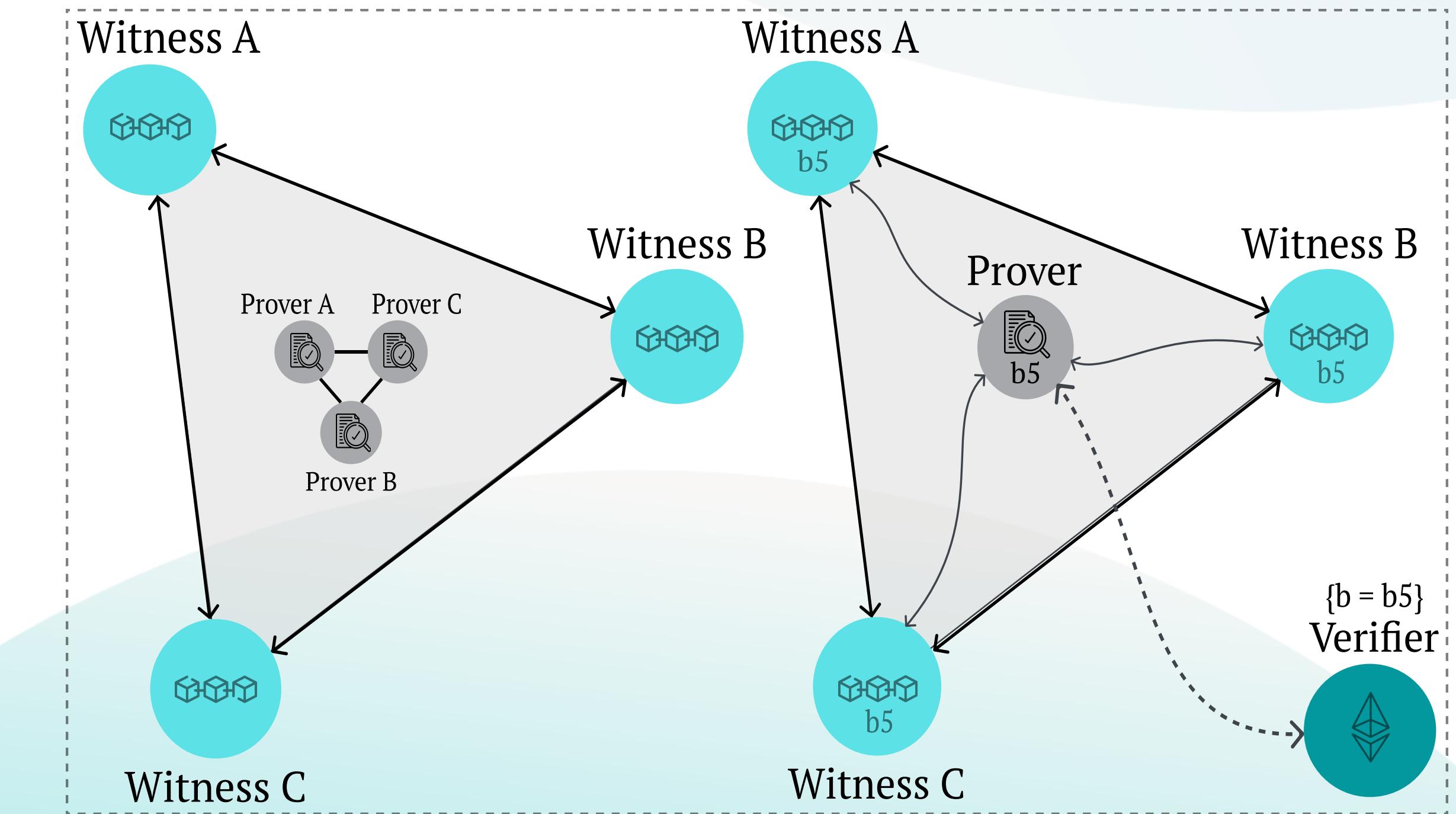


Turing-Complete Clock Synchronization

Permissionless Consensus Mechanisms

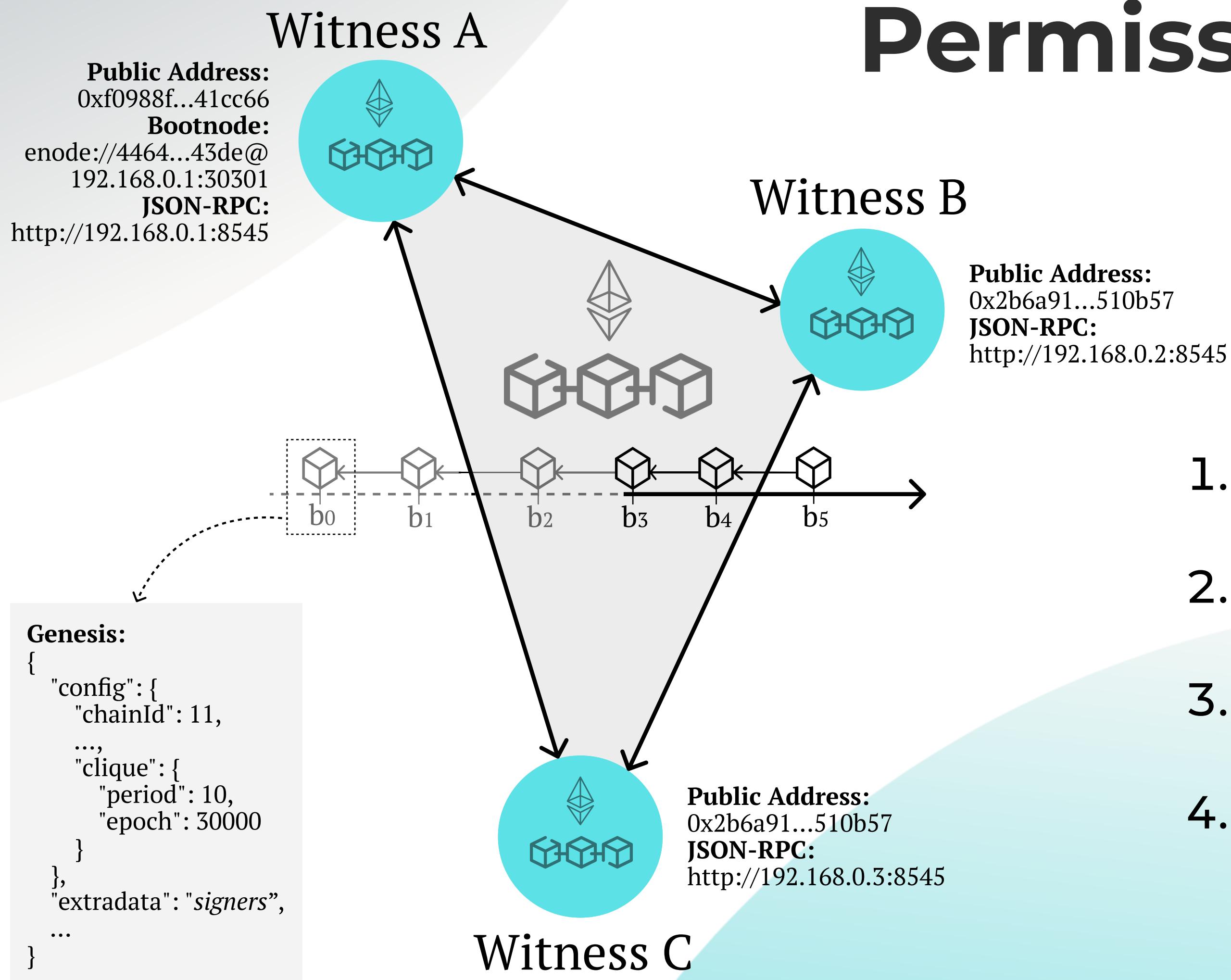


Zone-relative
Time Consciousness



Turing-complete
Smart Contracts

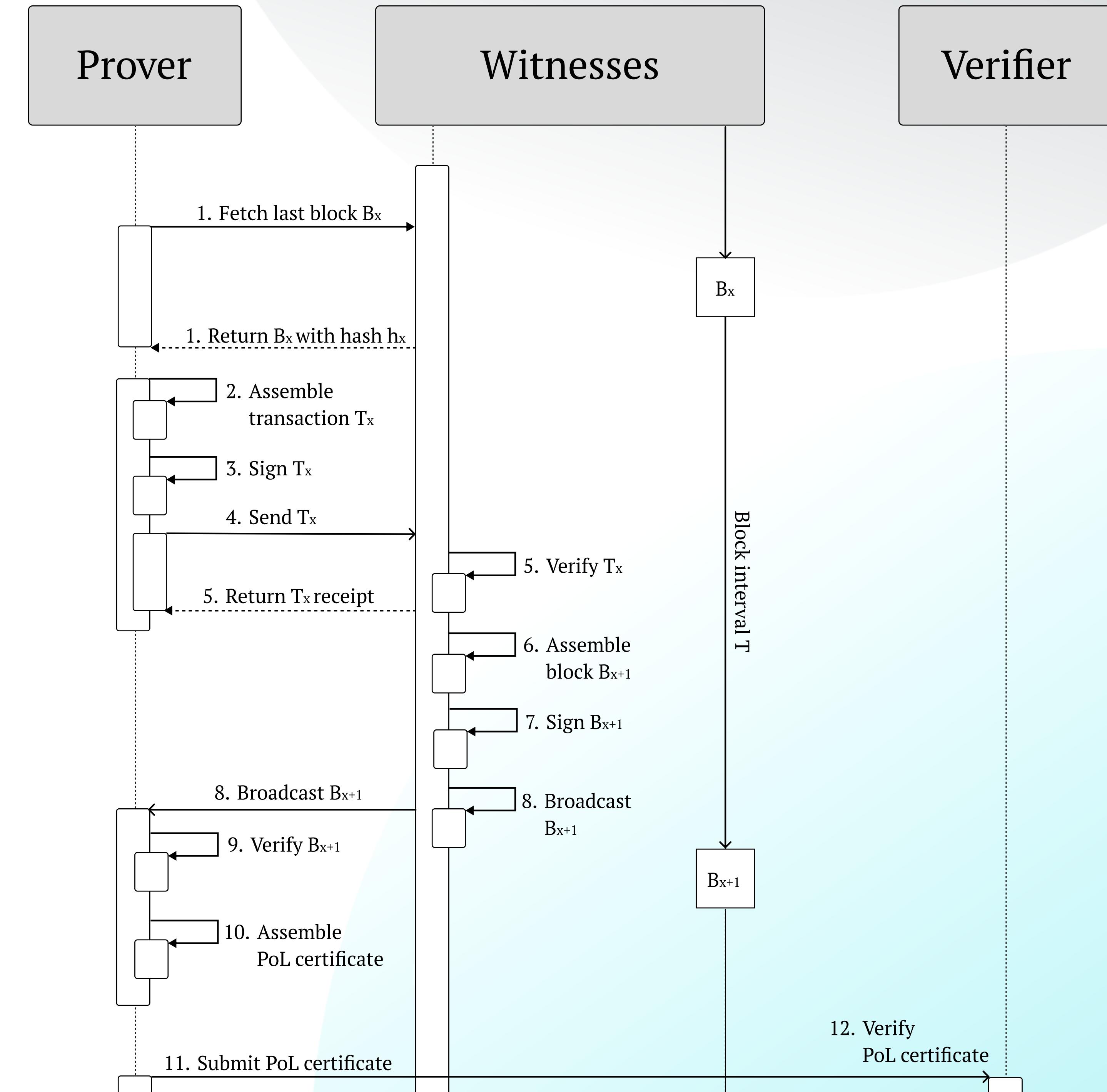
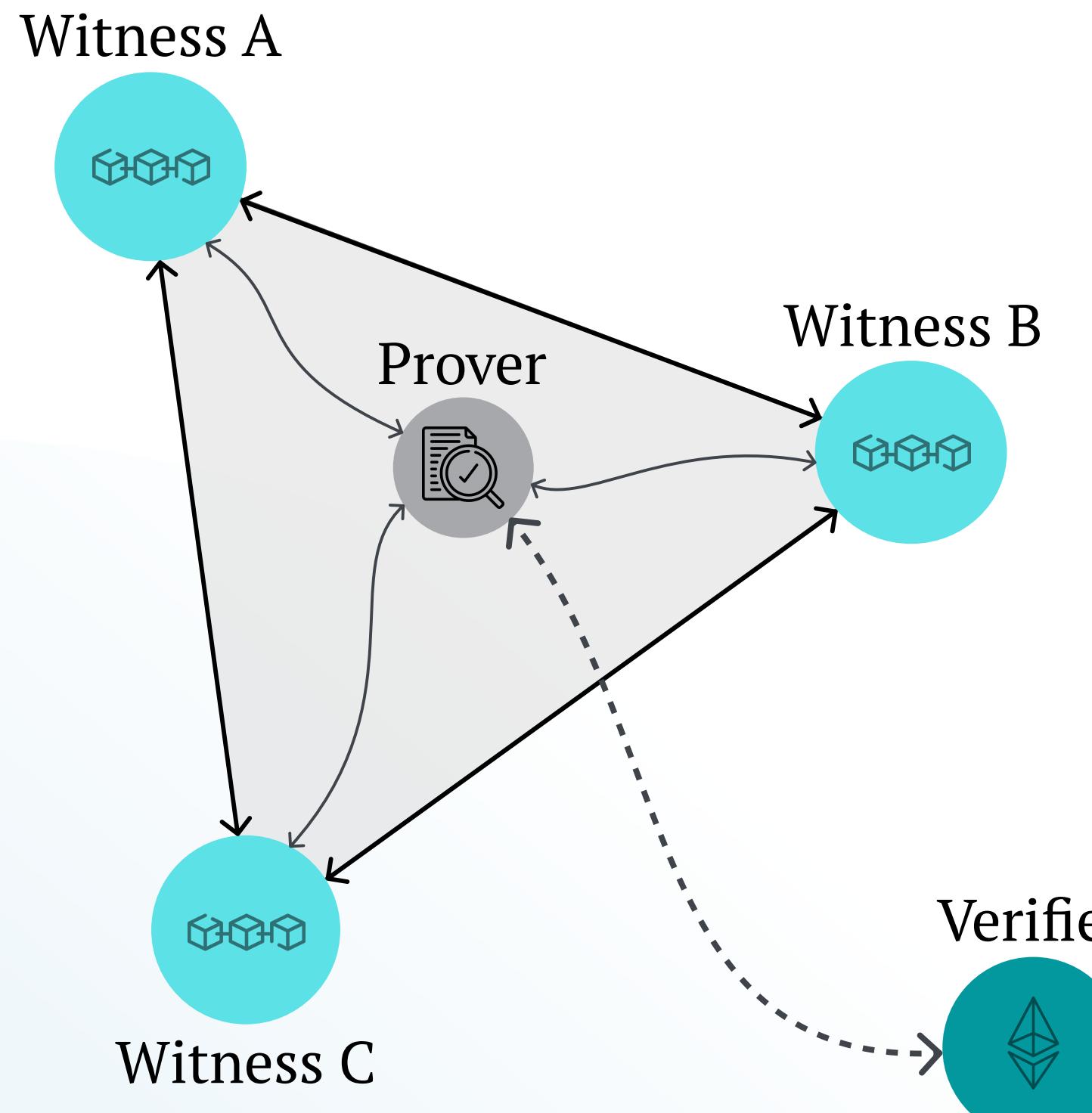
Practical Permissionless Consensus Ad-hoc Ethereum Network



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

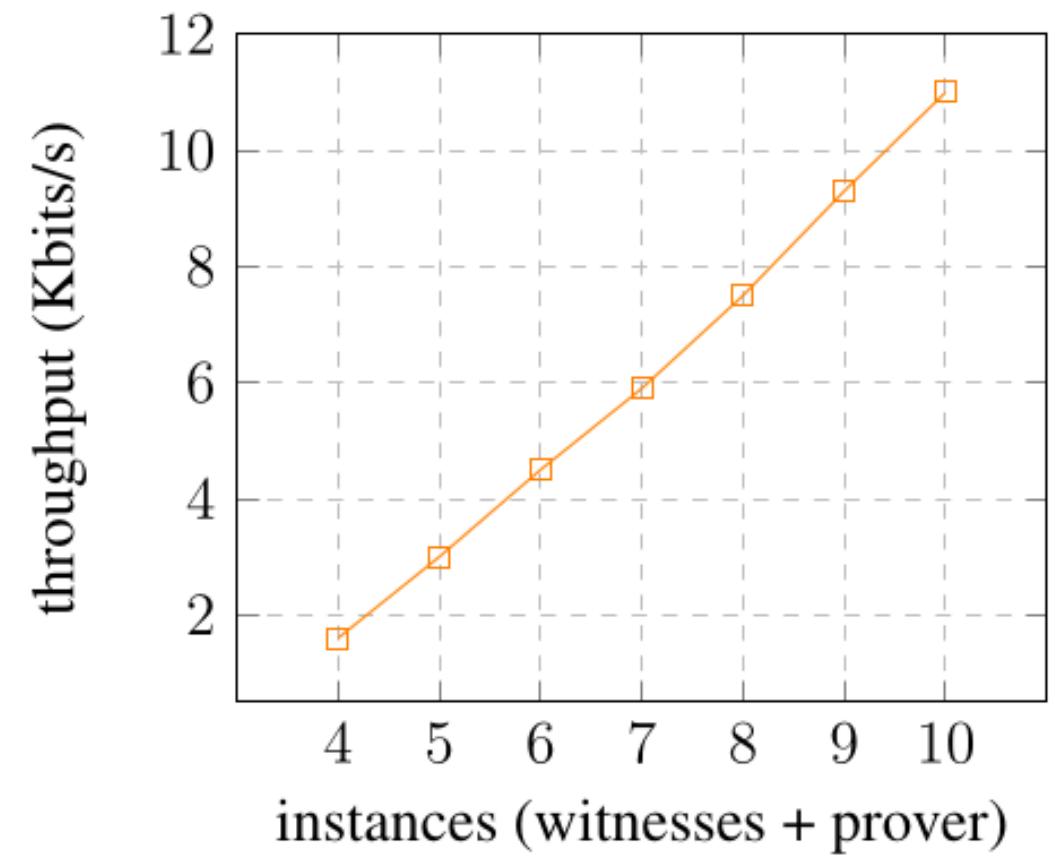
Proof Generation and Verification

Prover & Verifier Processes

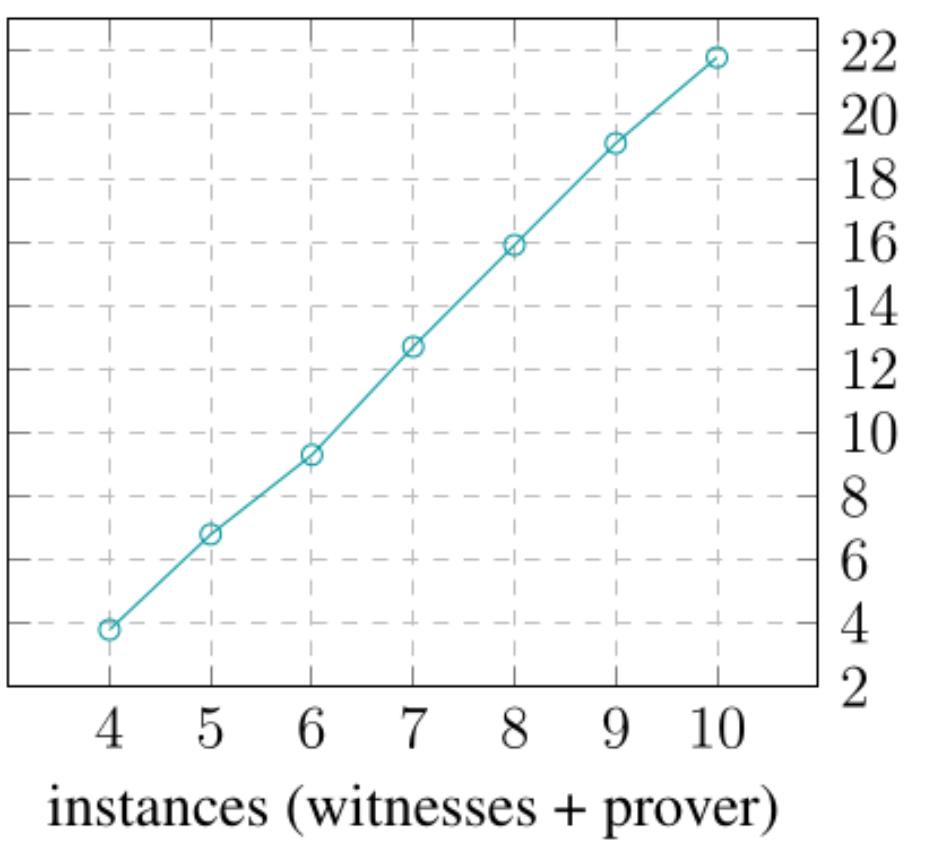


Performance Measurements

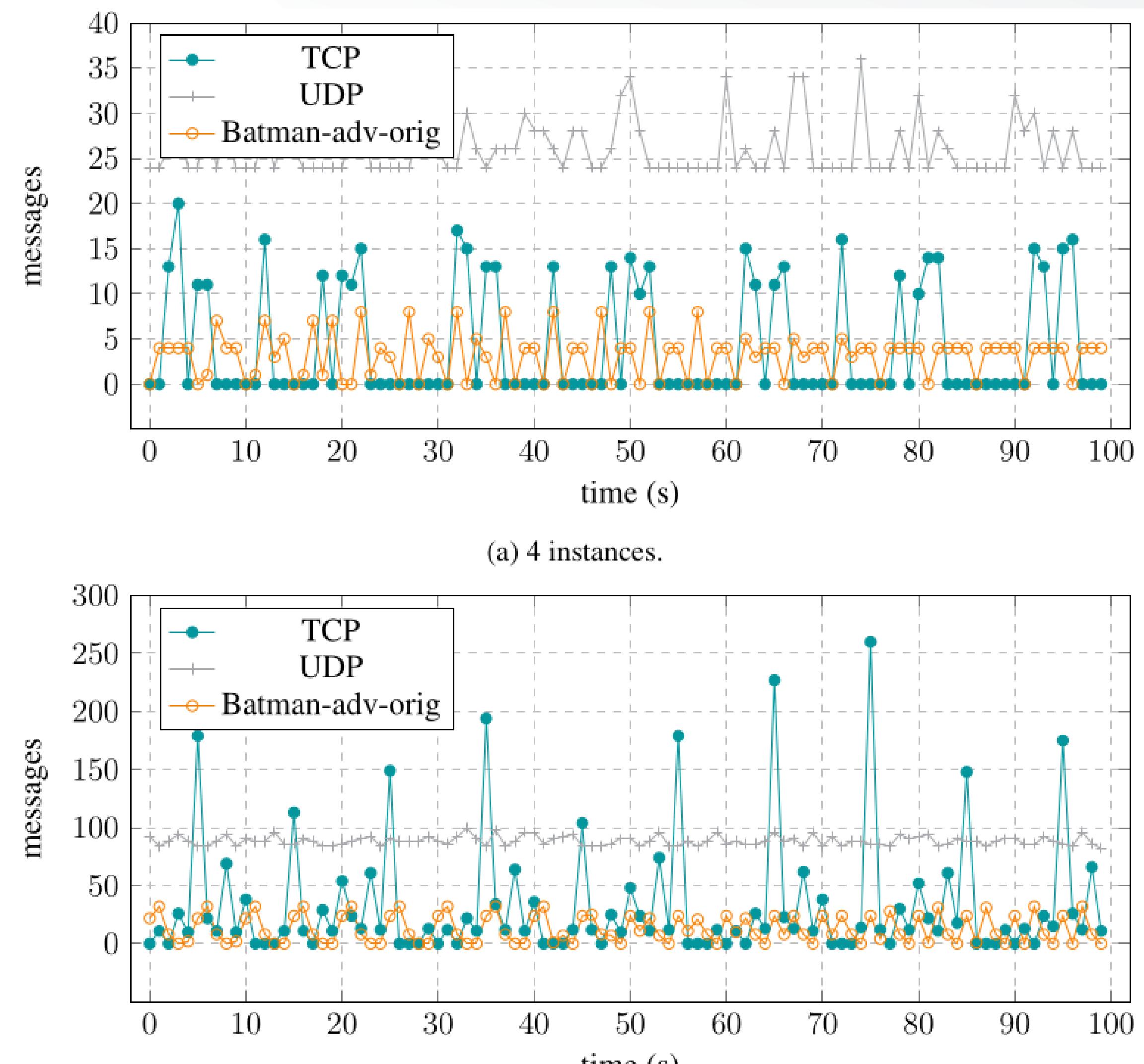
Protocols throughput



(a) Batman-adv traffic throughput.

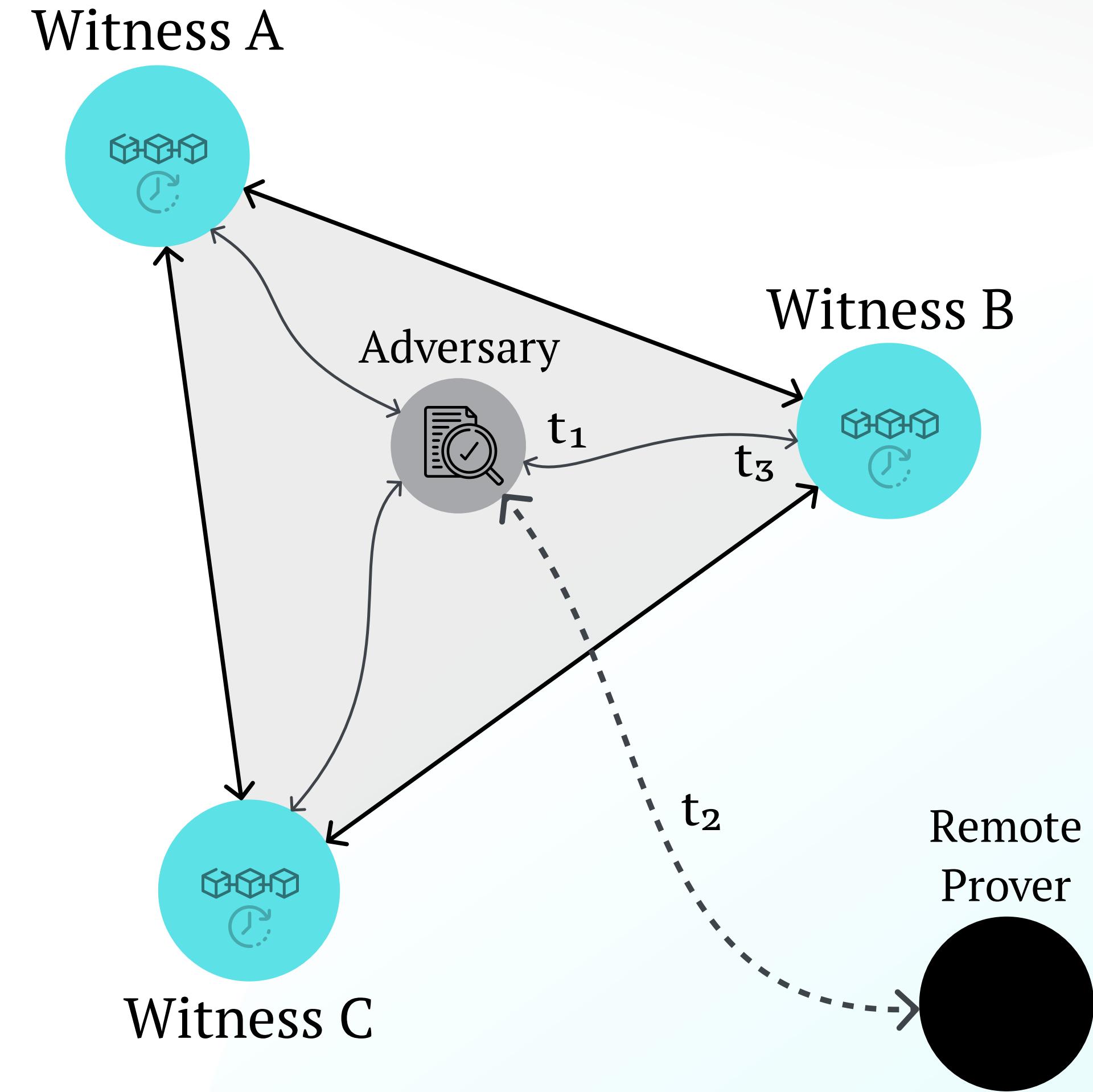
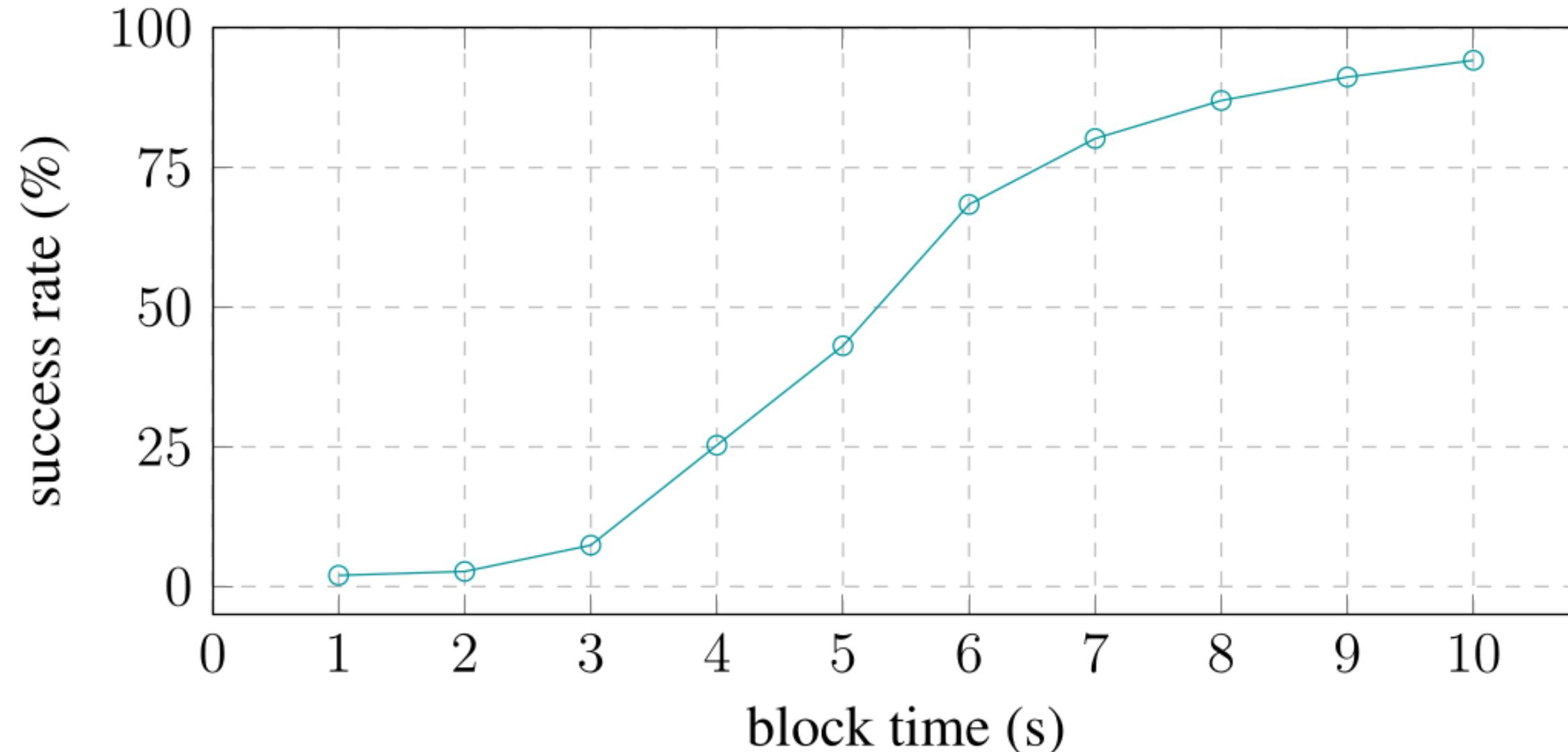


(b) IPv4 traffic throughput.



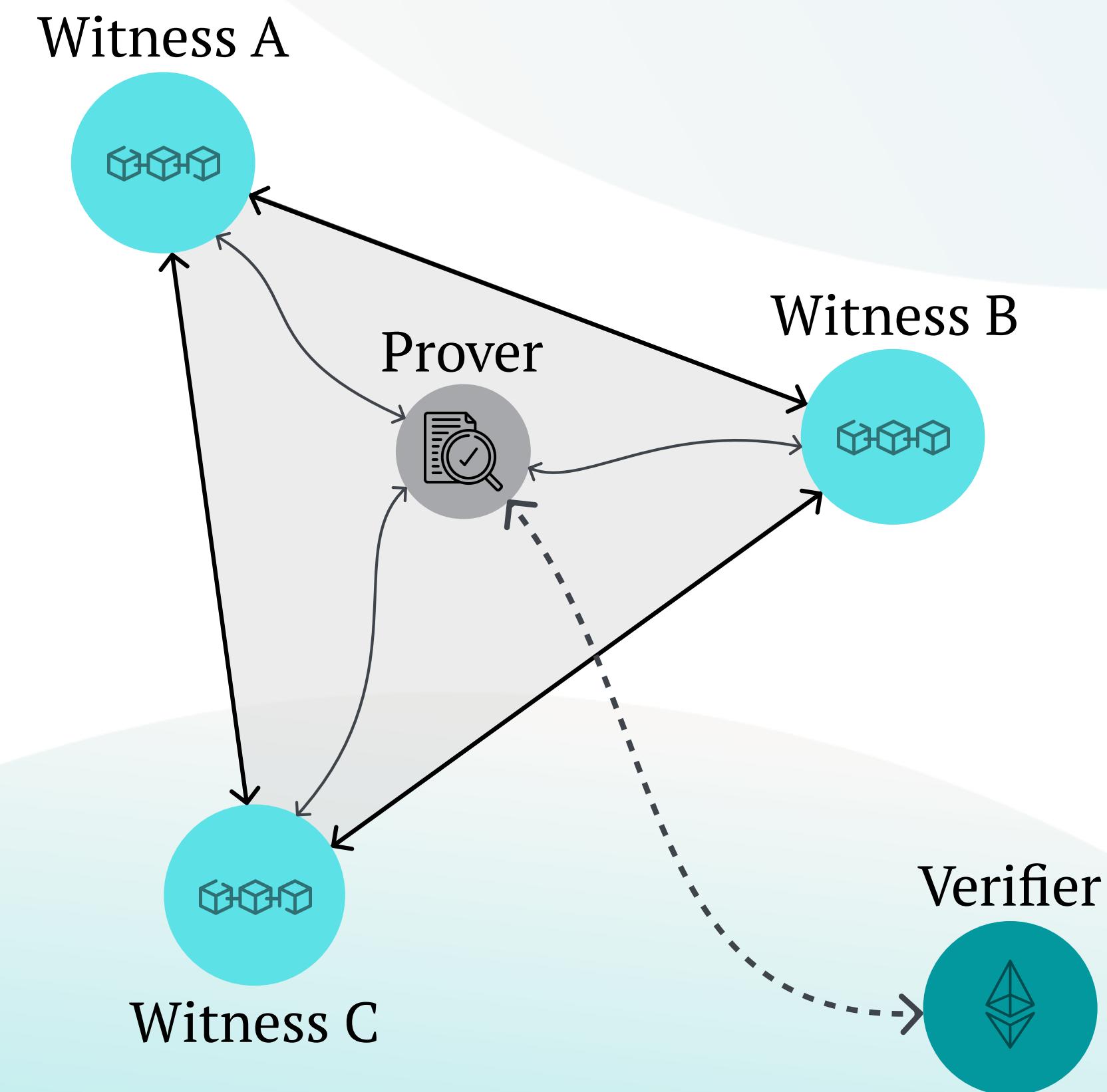
Success Rate and Attack Vectors

Block time and Proxy attacks



Future Work

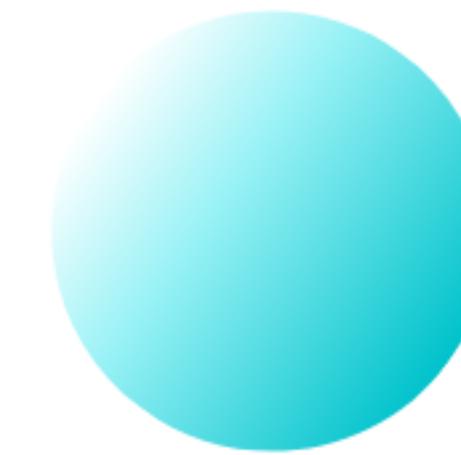
Smart Contracts
Identity Management Systems
Privacy Preserving Mechanisms
Consensus Protocols
Physical Deployment



20th of May 2023

Distributed Systems Seminar

Towards Decentralized Proof-of-Location



Eduardo Ribas Brito
Supervised by Ulrich Norbisrath

UNIVERSITY OF TARTU
Institute of Computer Science

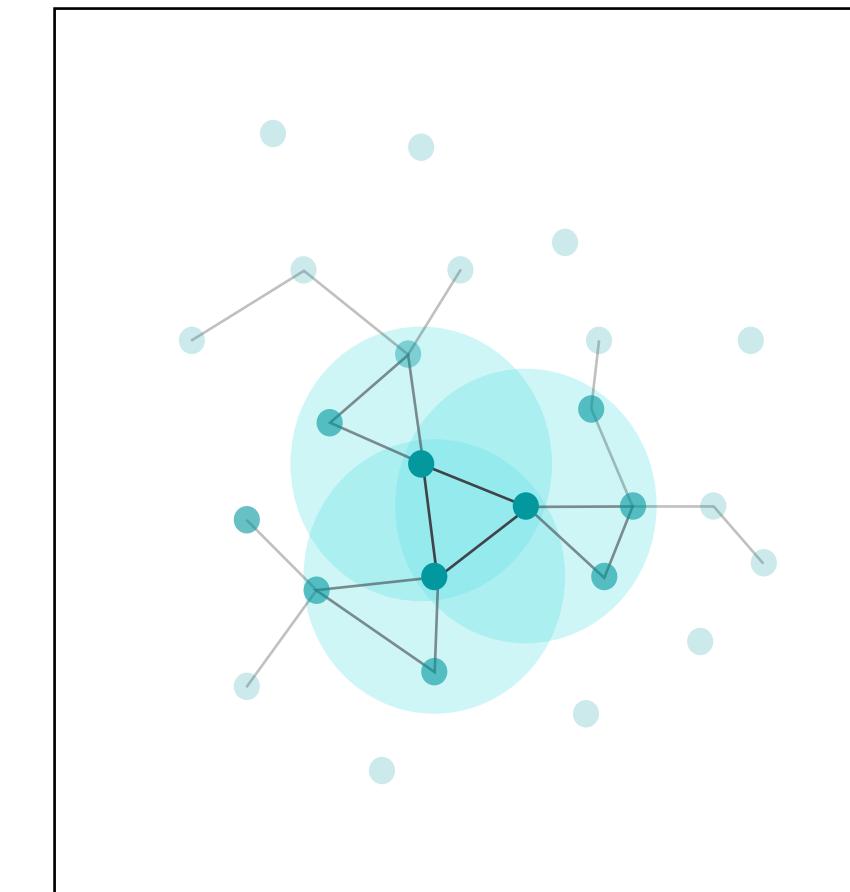
Appendix

Overview

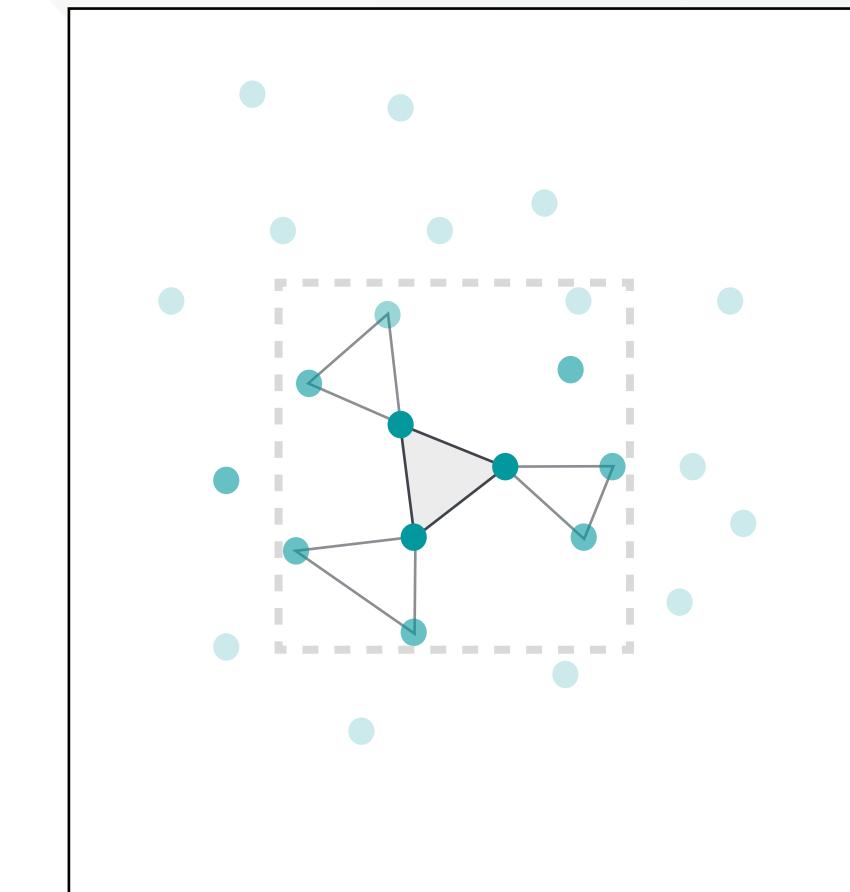
Protocol Fundamentals

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

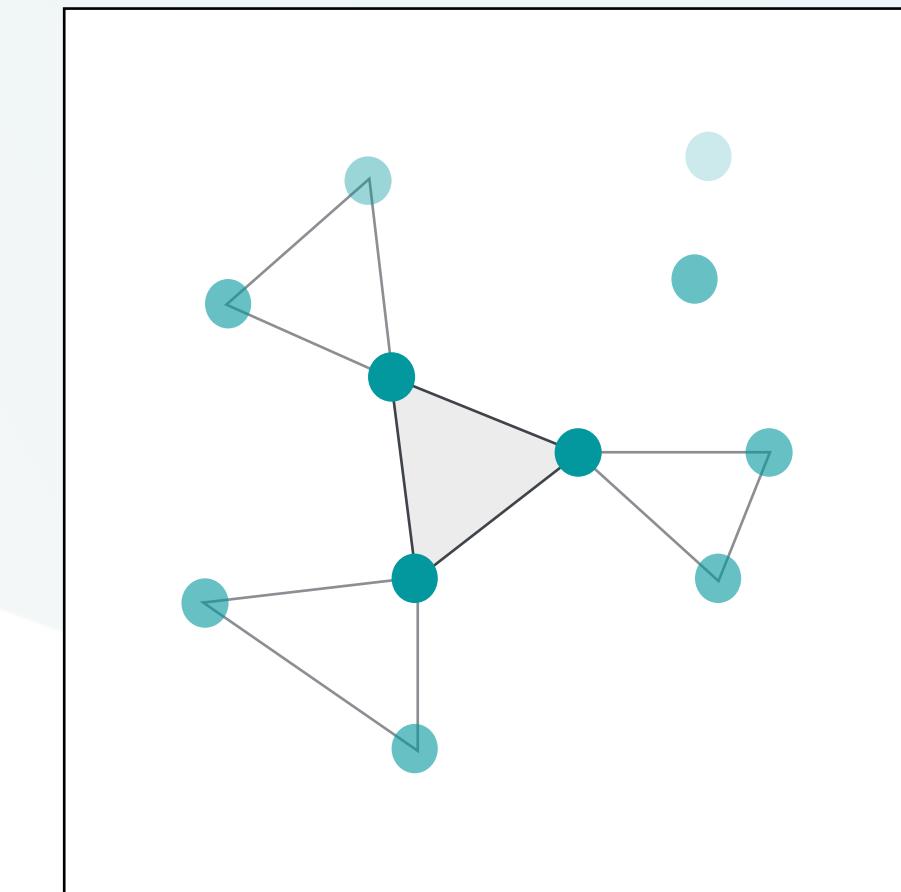
A. Mesh Network



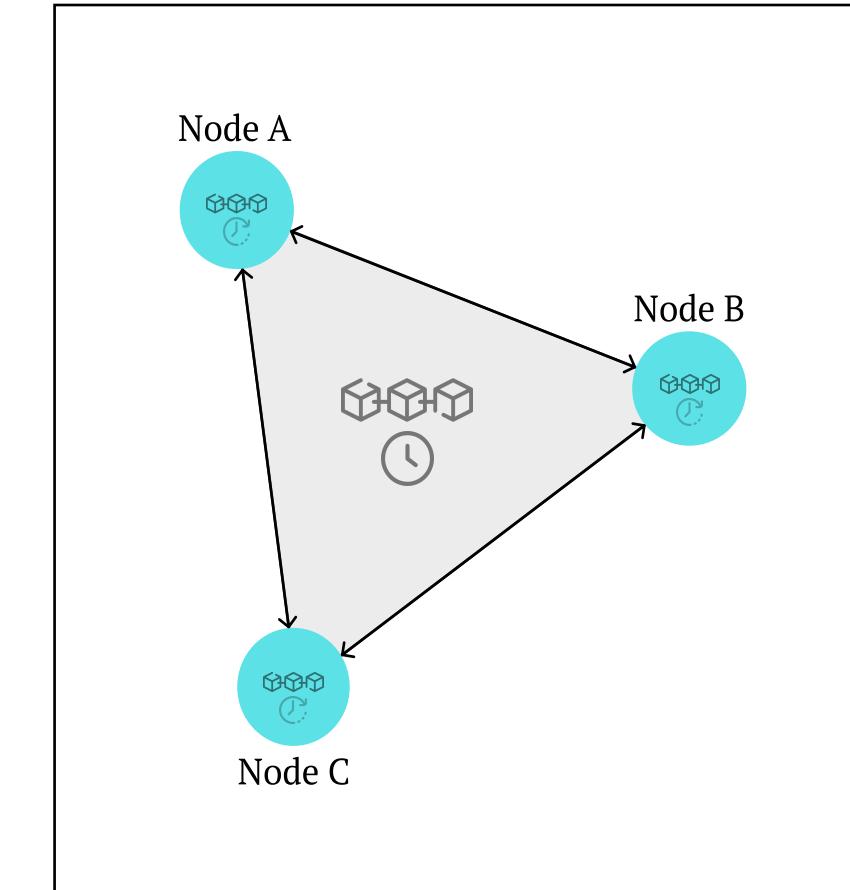
B. Zone Discovery



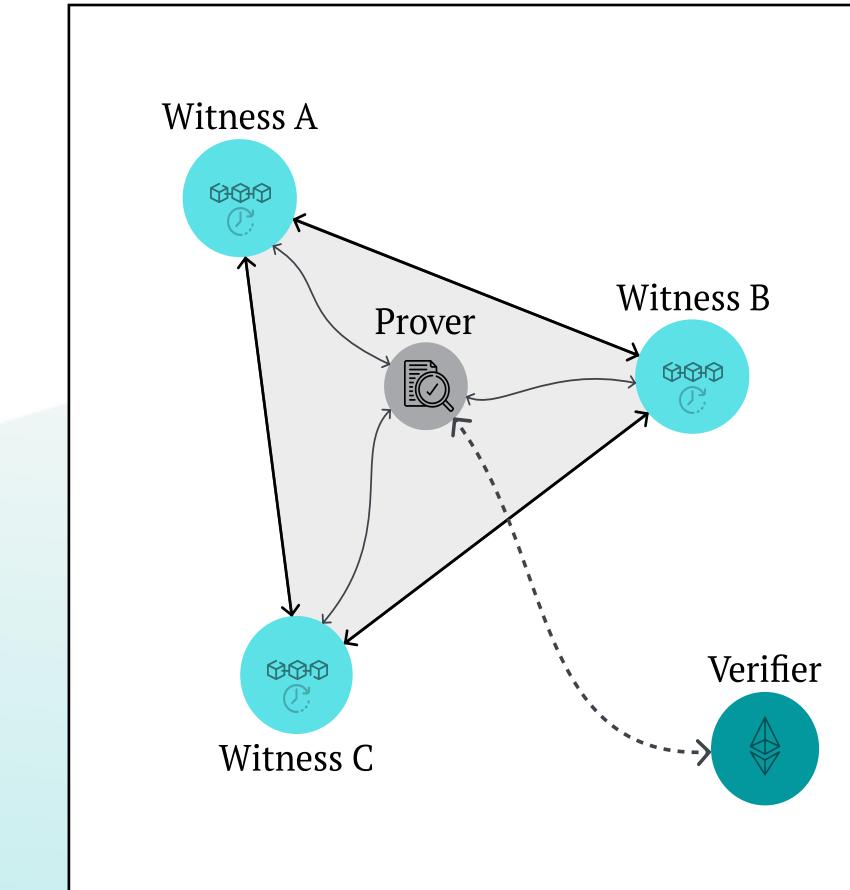
C. Zone Affinity



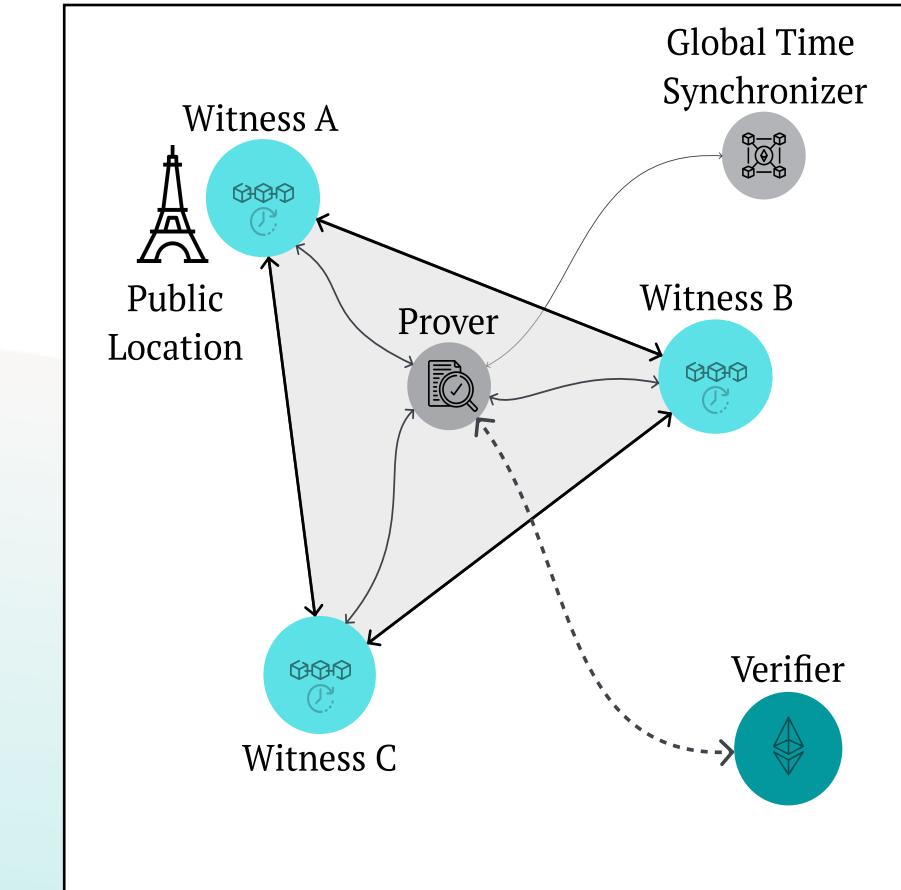
D. Zone Synchronization



E. Relative Proof-of-Location



F. Absolute Proof-of-Location

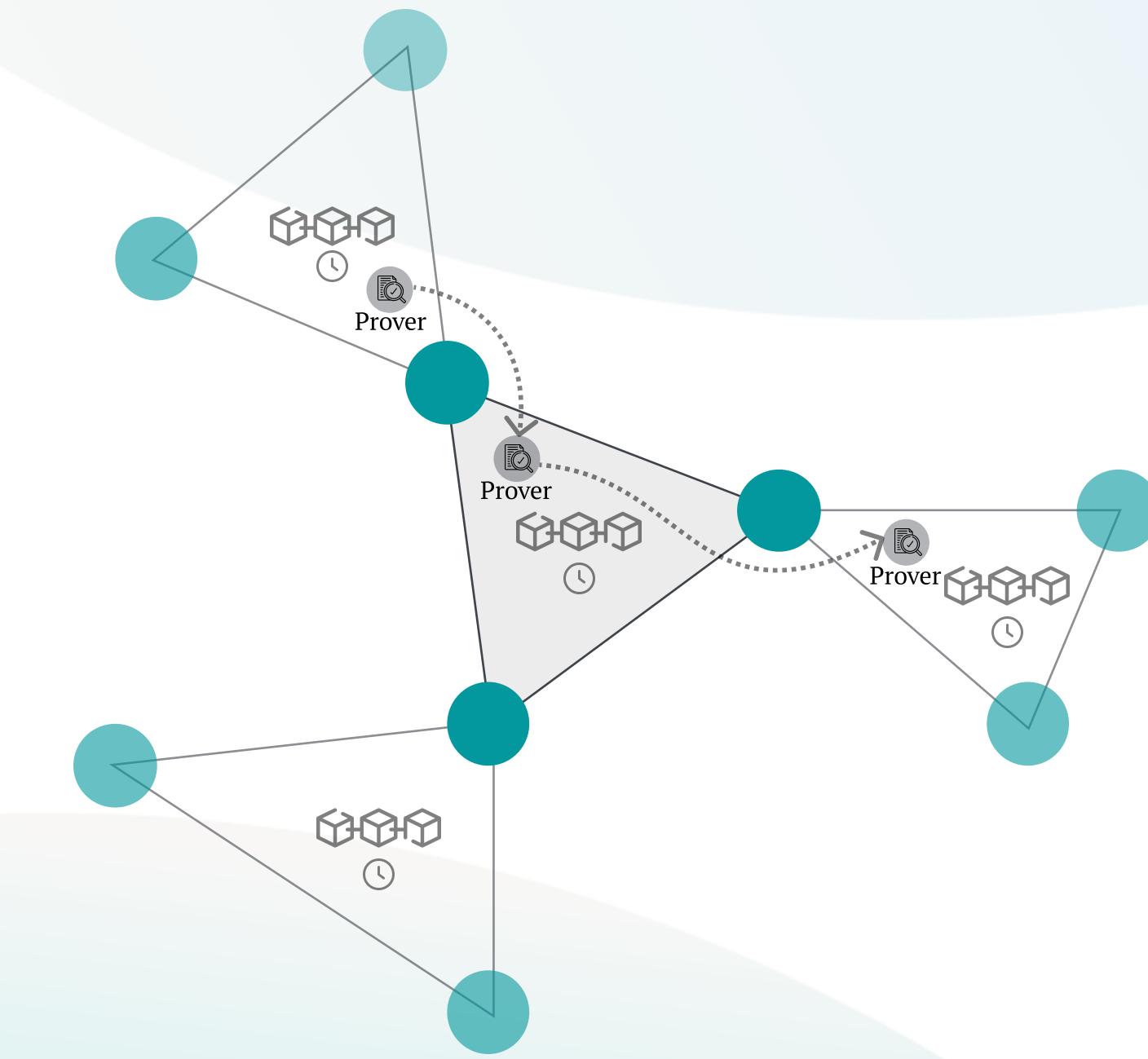
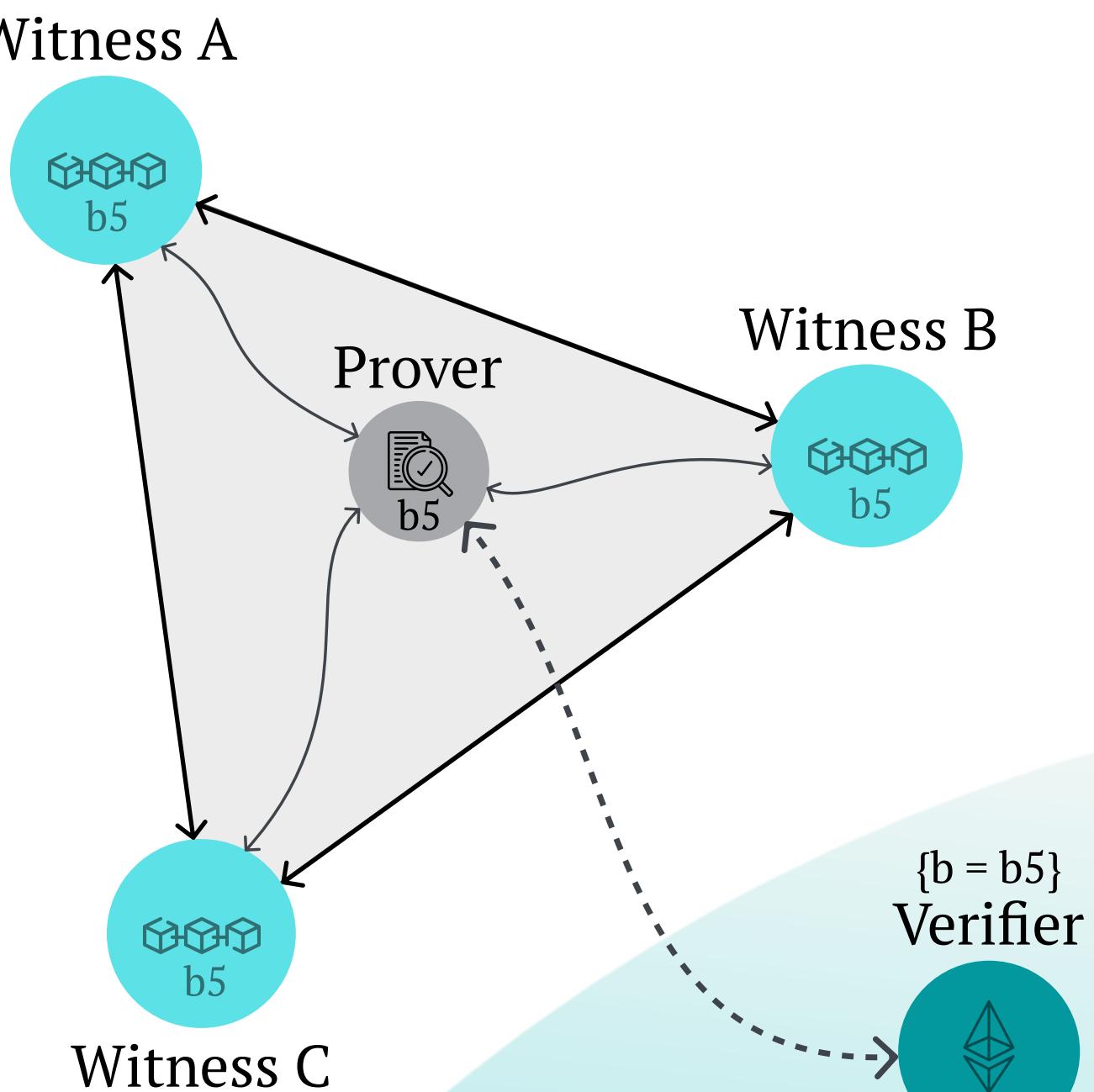
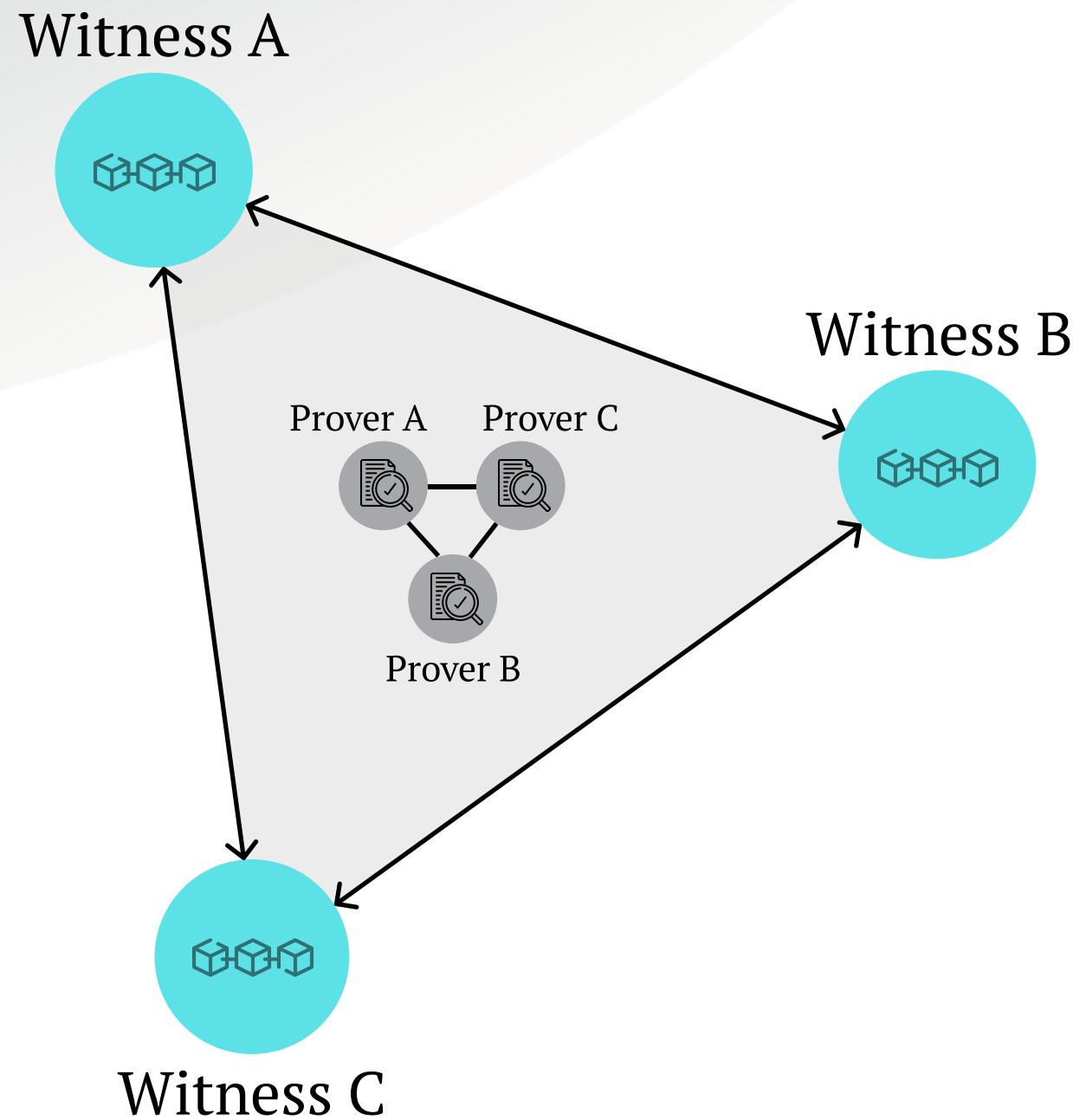


↔ short-range, synchronous communication

↔ long-range, asynchronous communication

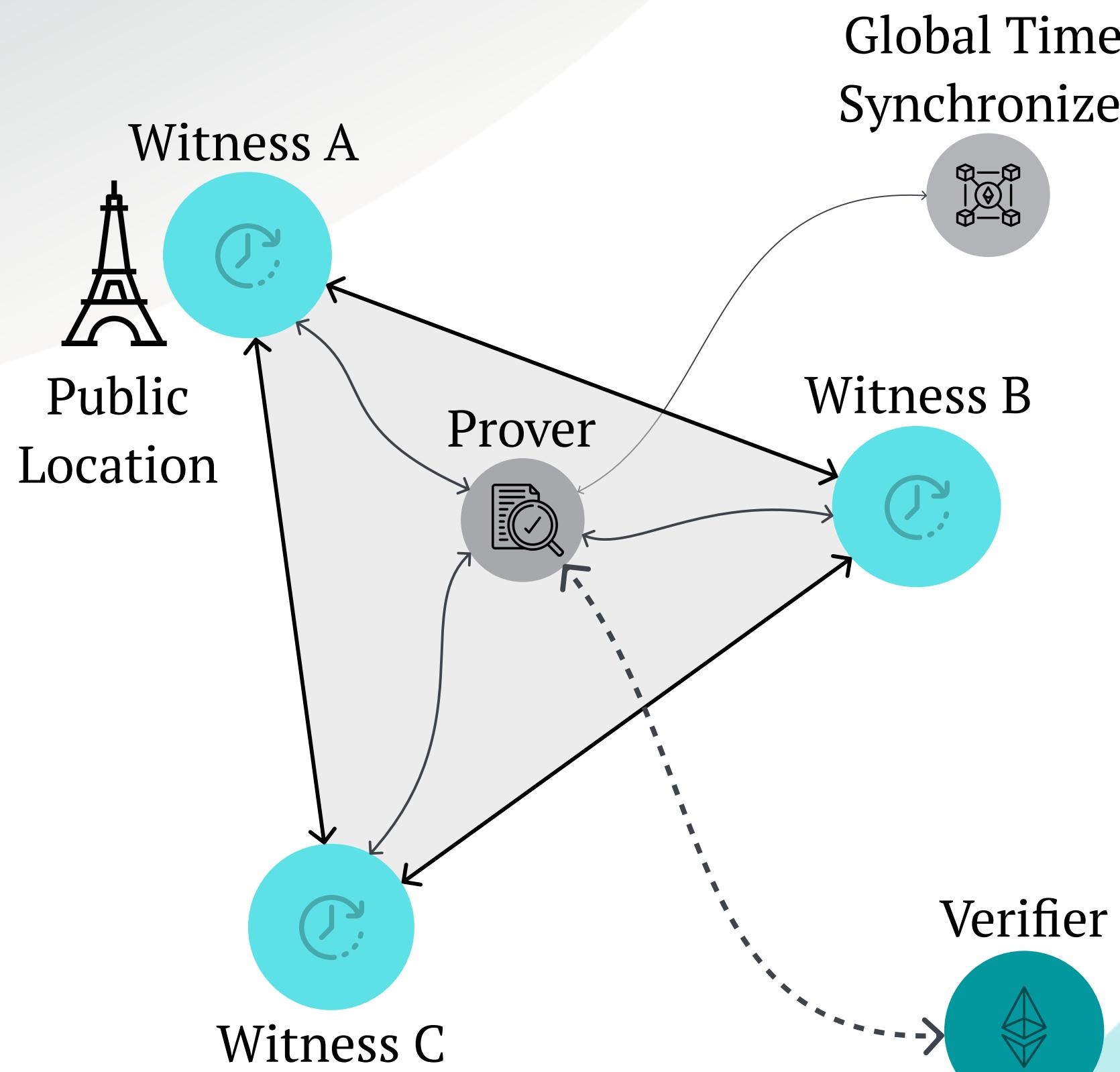
Smart Contracts

Turing-Completeness use cases



Absolute Proof-of-Location

From Relative Proof-of-Location



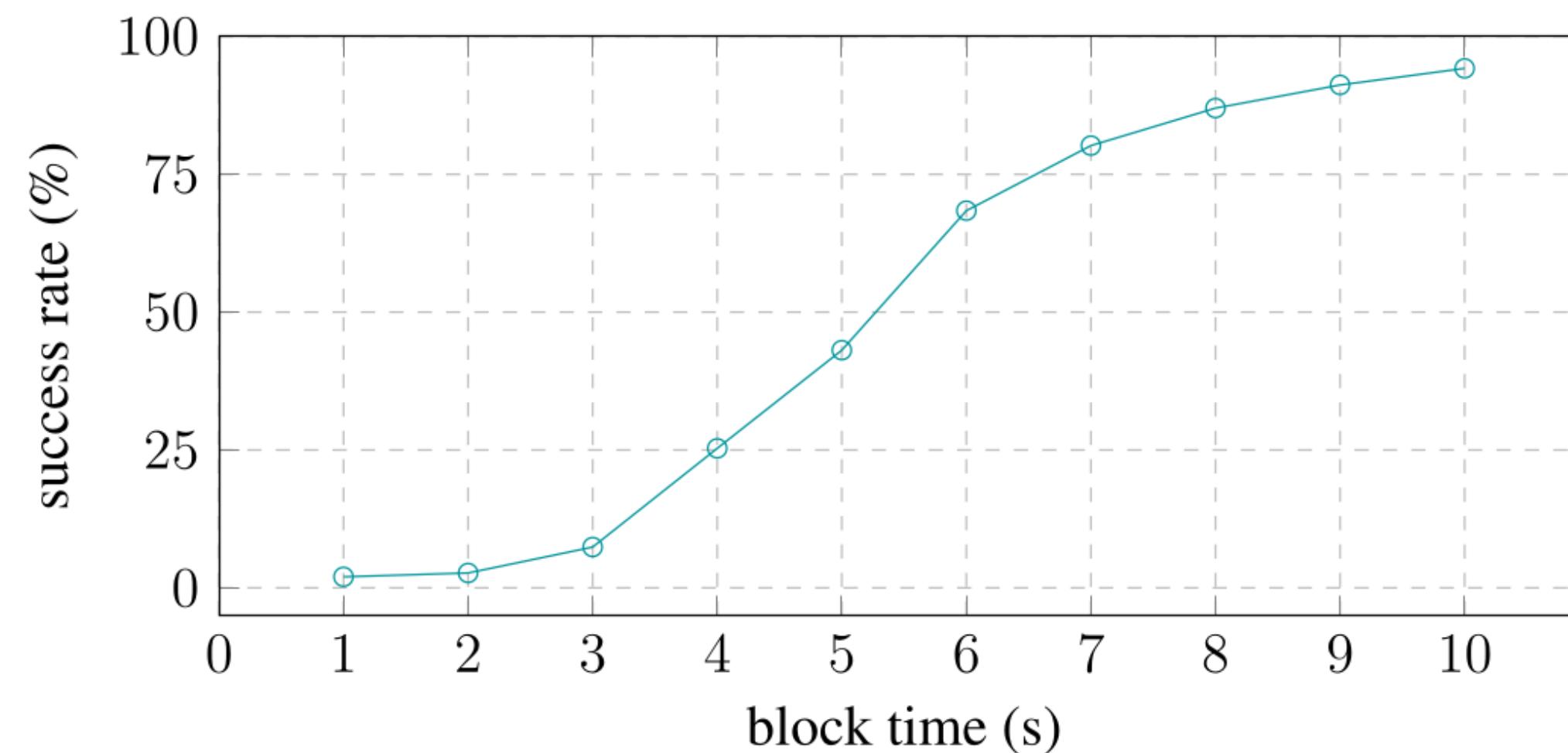
A Proof-of-Location certificate to be spatially and temporally acknowledged by any other node outside the zone needs:

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

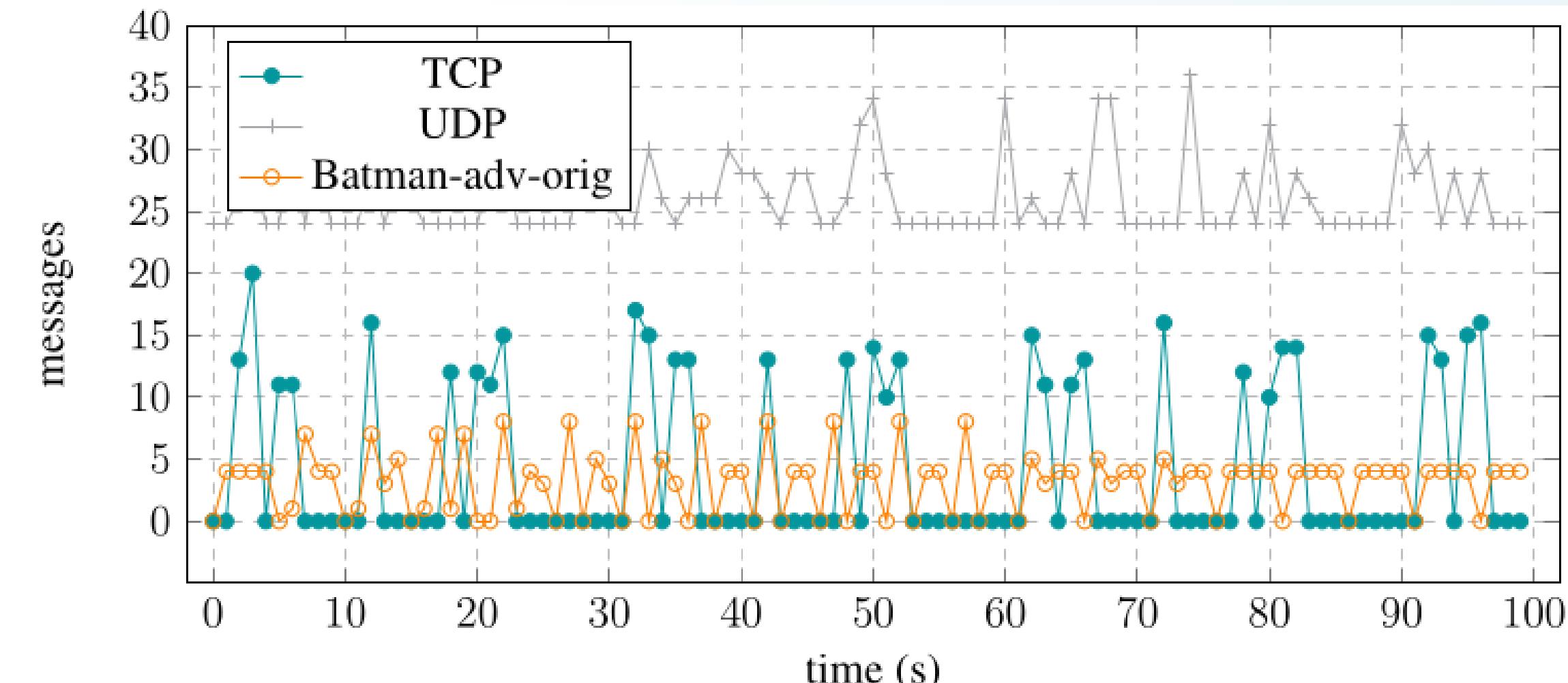
Measurements

Blockchain Activity & Success Rate

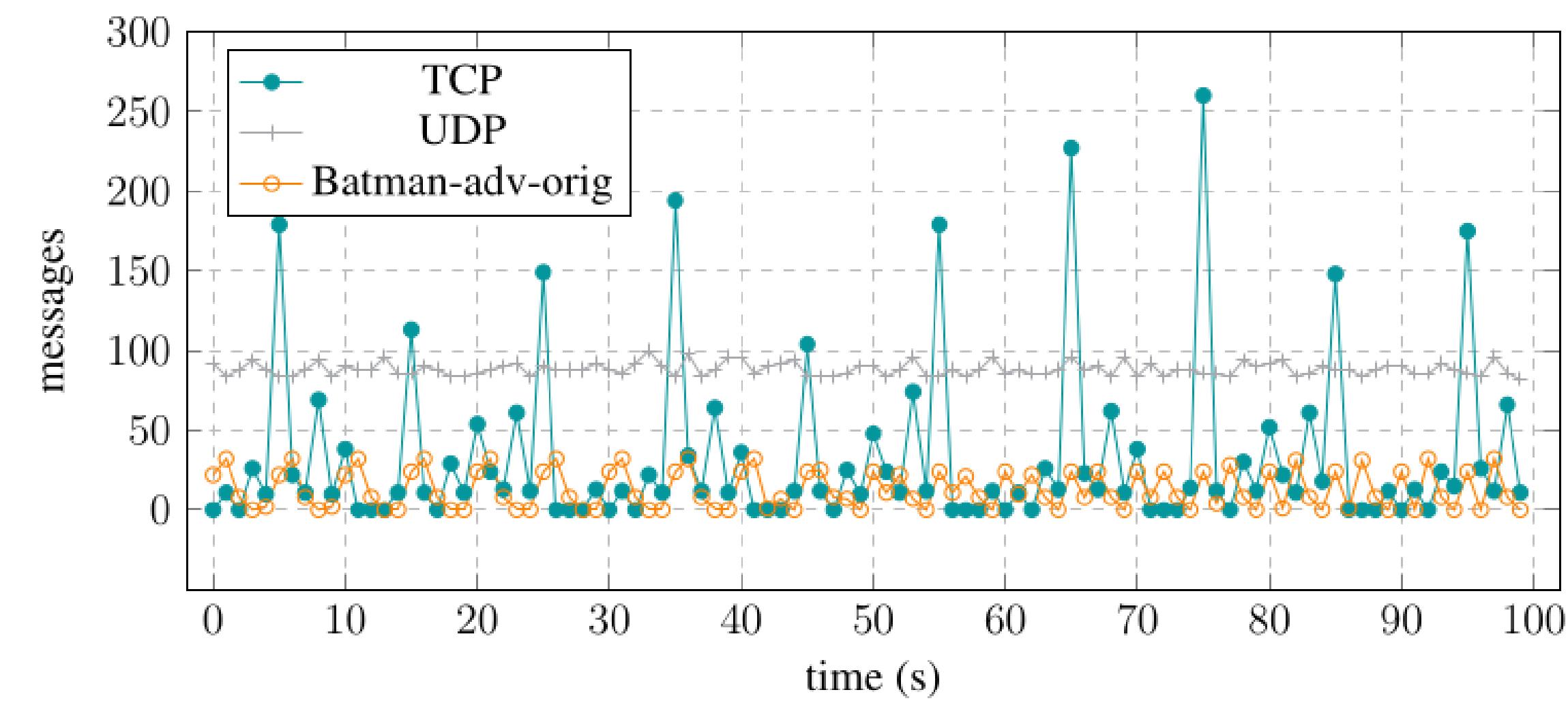
1. The interval time between blocks matches the higher peaks of TCP traffic, while the UDP traffic is more evenly distributed.
2. A more permissive block time allows for a lower number of invalid certificates, but also for a higher probability of witnessing malicious activity.



19



(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:

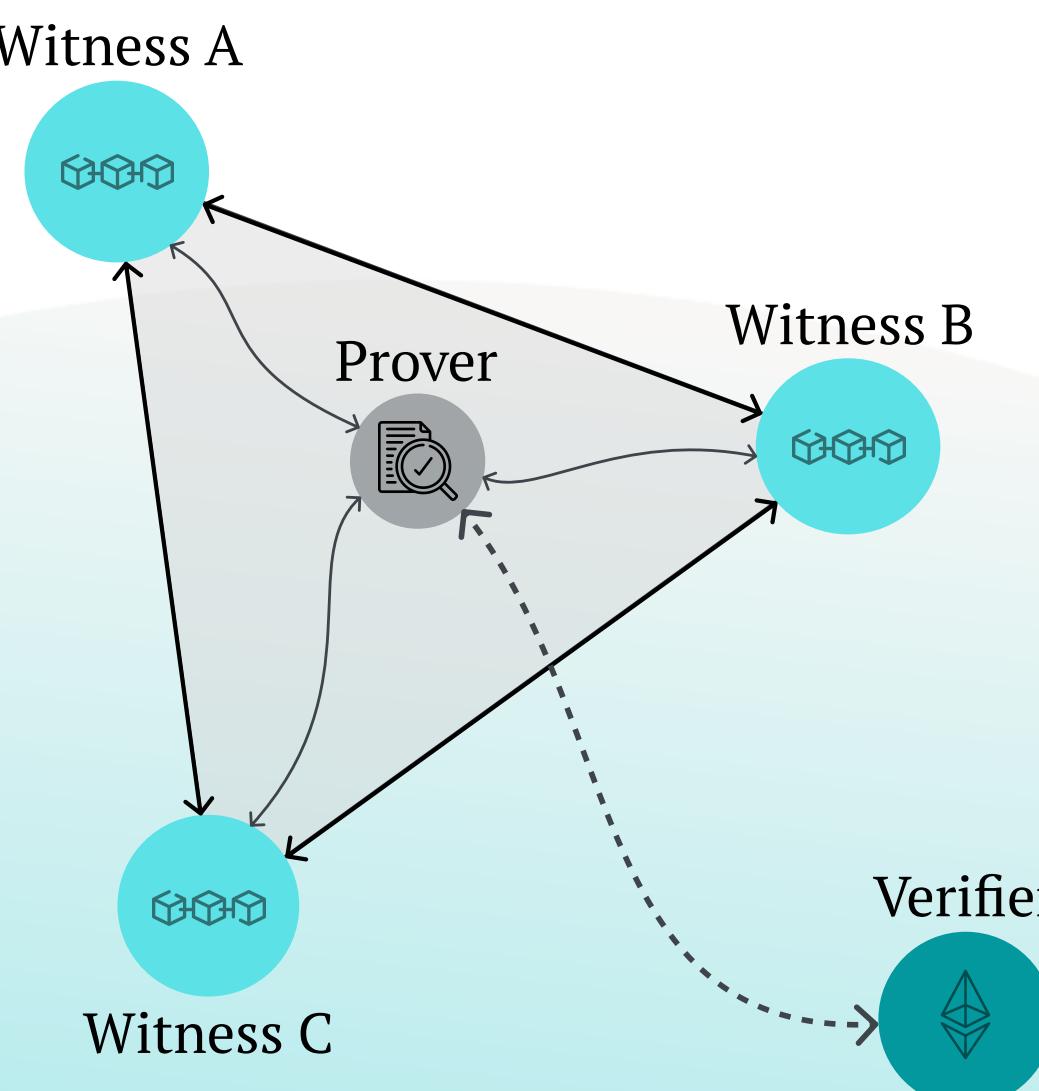
- a. Making full use of the system's Turing completeness for more complex logic

4. Protocol Extensibility:

- a. Integration of privacy preserving mechanisms, such as zero-knowledge proofs

5. Physical Deployment:

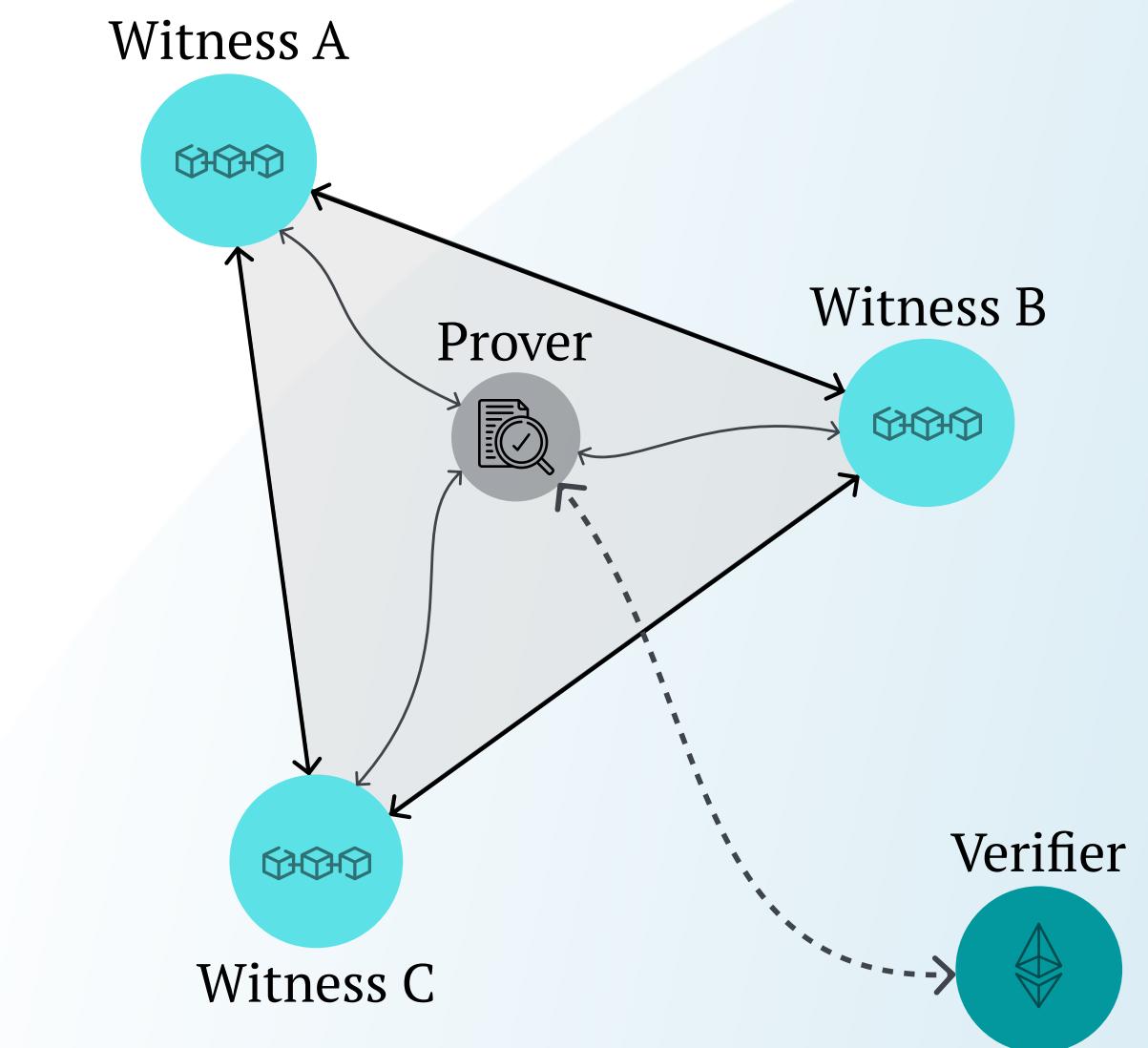
- a. And the evaluation of the performance in real-world scenarios



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 Nobisrath

UNIVERSITY OF TARTU
Institute of Computer Science