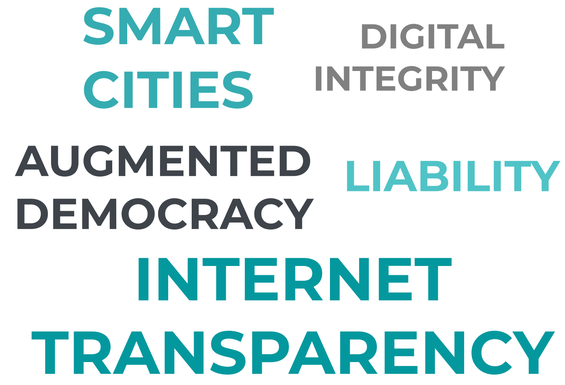
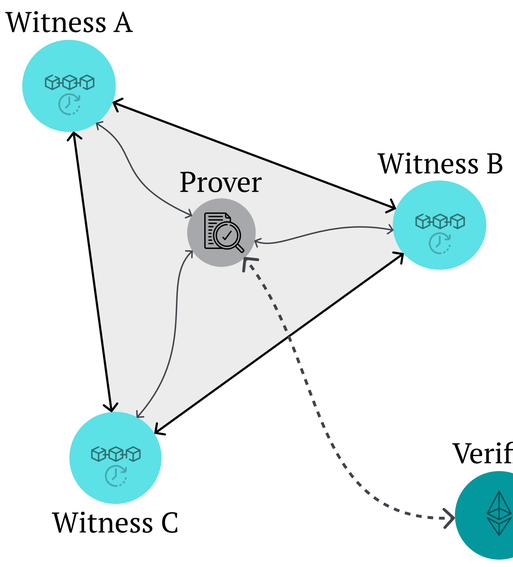
Towards Decentralized Proof-of-Location

Authored by Eduardo Brito
Supervised by Ulrich Norbisrath

UNIVERSITY OF TARTU
Institute of Computer Science
XRP Ledger Foundation
European Union, European Social Fund — Investing in your future

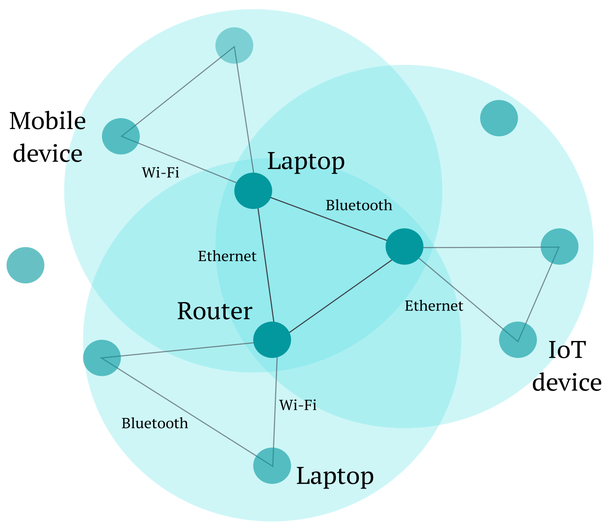




A digital Proof-of-Location is an electronic certificate that attests one's position in both space and time.

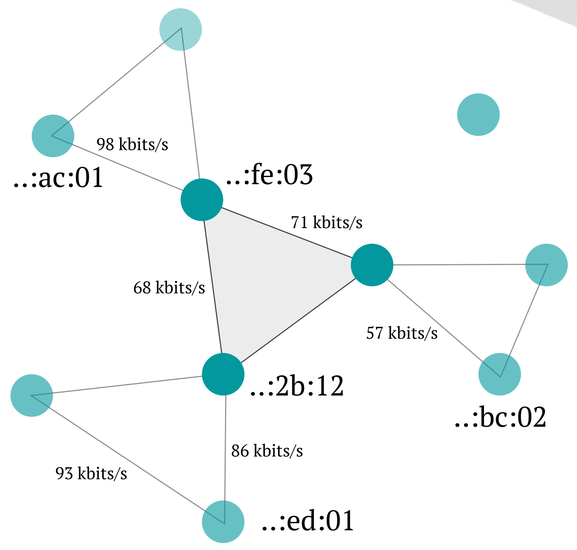
A ***prover*** engages in a communication protocol with nearby participants, the ***witnesses***, with the goal of gathering a verifiable Proof-of-Location claim, to be later presented to a ***verifier***, convincing it of one's existence within a geographical area, at a given moment.

1. Dynamic Mesh Networks

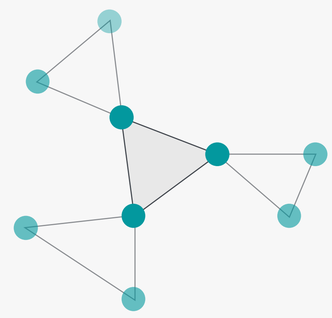


In mesh topologies, nodes are directly and dynamically connected, in a **non-hierarchical** way. This trait allows for many-to-many communications between devices, to efficiently route the data. The mesh nodes are expected to **dynamically** self-organize and self-configure.

Mesh networks enable short-range wireless exchange of messages, leading to space synchronization.



Space Synchronization



+

Time Synchronization

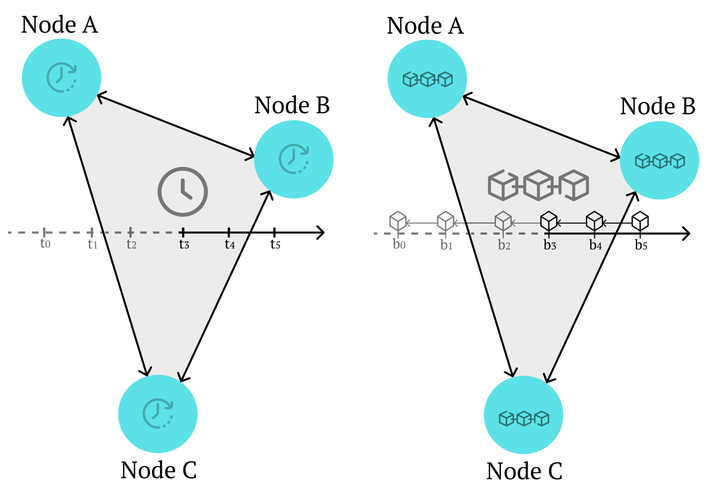
=

Trustless Proof-of-Location

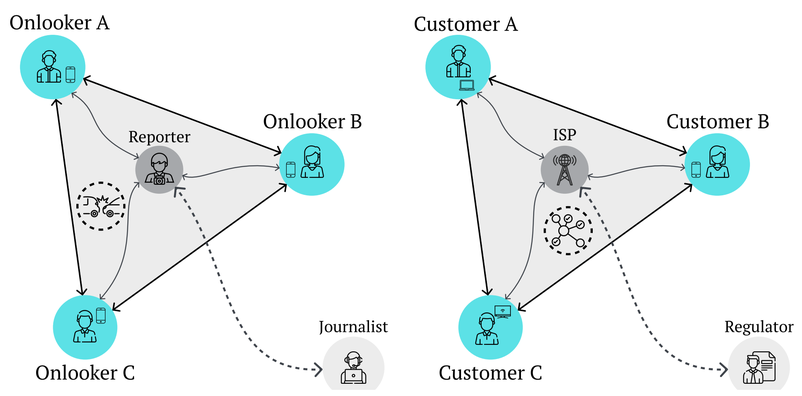
2. Permissionless Consensus

In **decentralized and trustless** environments, achieving time synchronization

is the problem of achieving permissionless consensus, and the need for **ordering and synchronizing** events at the same pace, when participants are **not necessarily trusted**. Permissionless consensus with a Turing Complete environment enables location-based **smart contracts**.



3. Verifiable Proof-of-Location



Agreeing on a location, short-range communication, and internal clock synchronization, we can now generate

complete and spatio-temporally sound location claims, achieving decentralized Proof-of-Location.

The verification process only needs the nodes' public keys and the Proof-of-Location certificate, just like any **digital signature verification**, integrated with applications of all kinds.

Public repository:
https://github.com/edurbrito/proof-of-location

Acknowledgements to Eero Vainikko and the participants of the Distributed Systems Seminar.