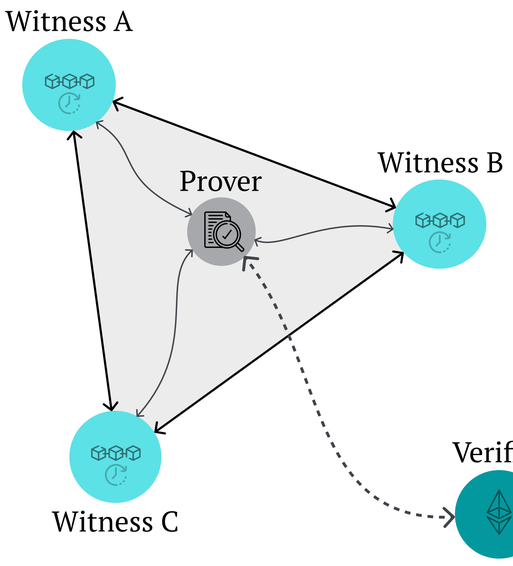
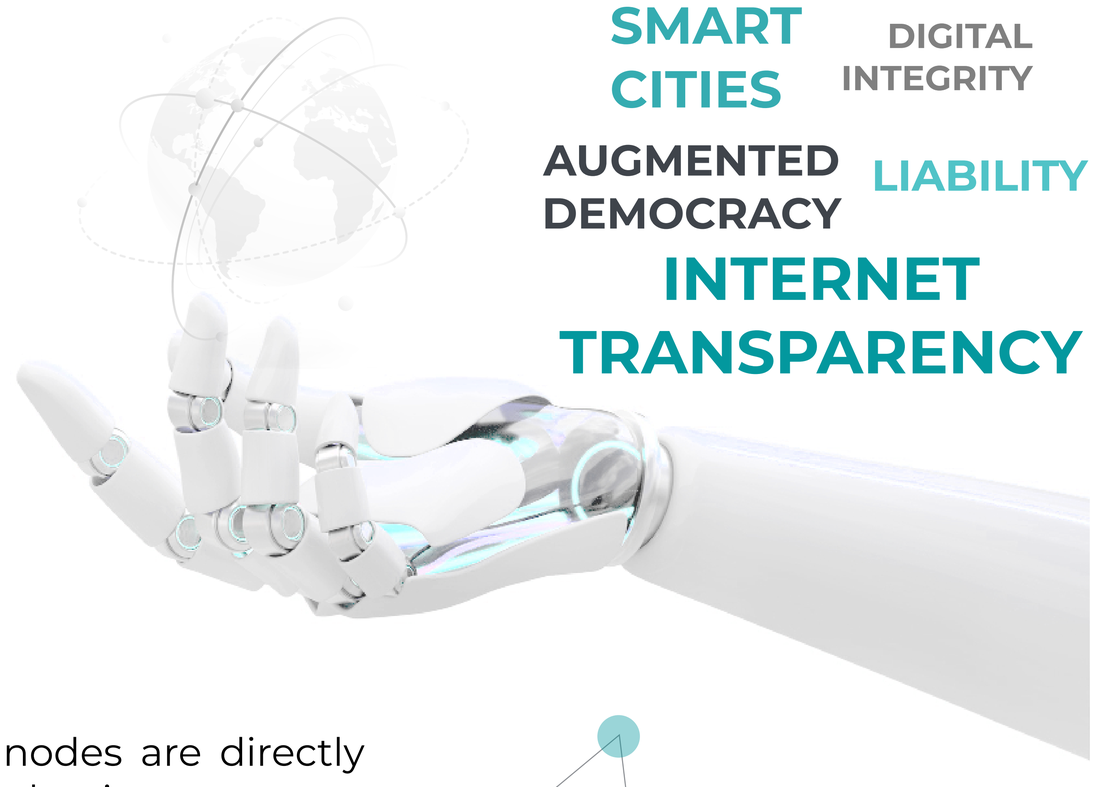
Towards Decentralized Proof-of-Location

UNIVERSITY OF TARTU
Institute of Computer Science
XRP Ledger Foundation

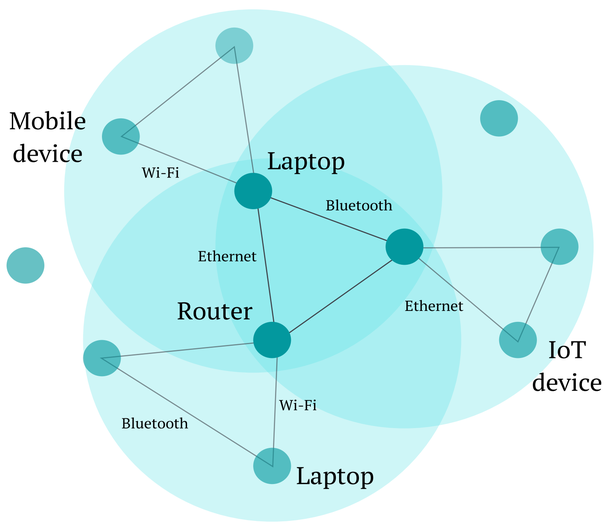


A digital Proof-of-Location is an electronic certificate that attests one's position in both space and time.

These location-proof arrangements expect the existence of a ***prover*** that engages in any 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***, therefore convincing it of one's existence within a geographical area, at a given moment.

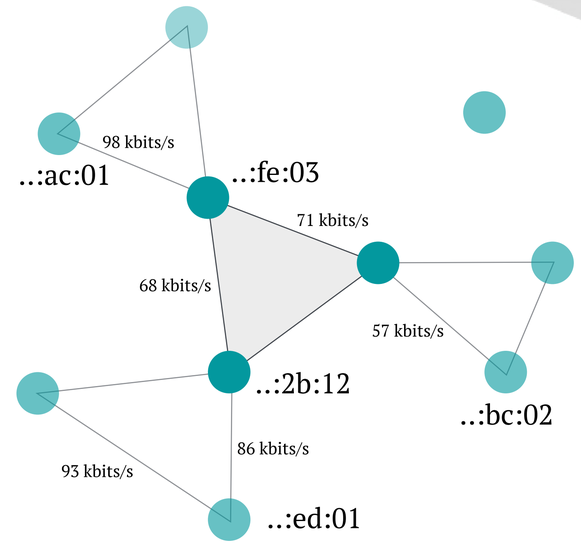


1. Dynamic Mesh Networks

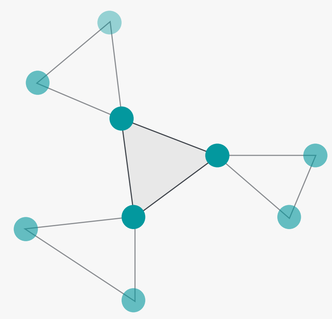


In mesh topologies, network nodes are directly and dynamically connected, in a **non-hierarchical** way. This trait allows for many-to-many communications between the devices, to efficiently route the data. The nodes that make up the mesh are expected to **dynamically** self-organize and configure themselves.

Mesh networks enable **short-range** wireless exchange of messages between the participants of a Proof-of-Location protocol, leading them to reach **space synchronization**.

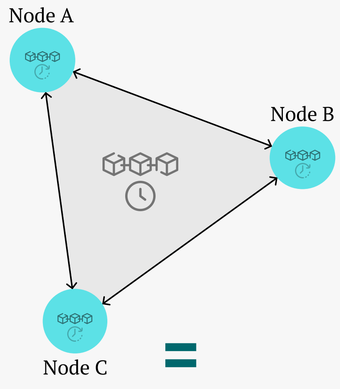


Space Synchronization



+

Time Synchronization



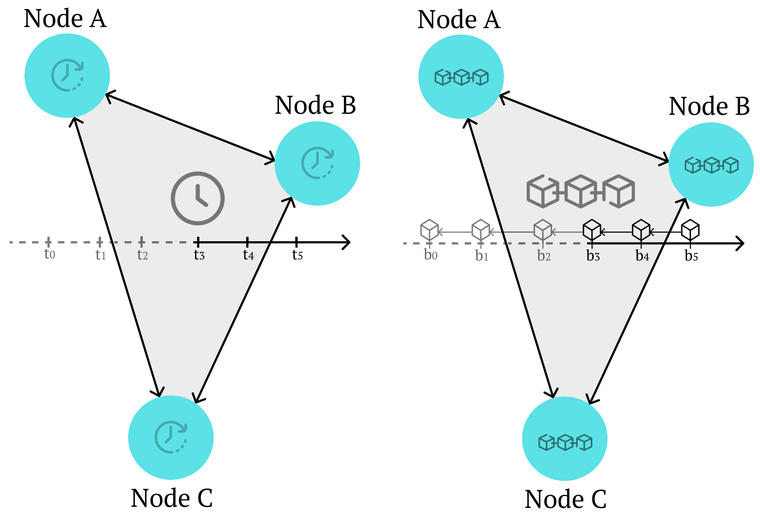
=

Trustless Proof-of-Location

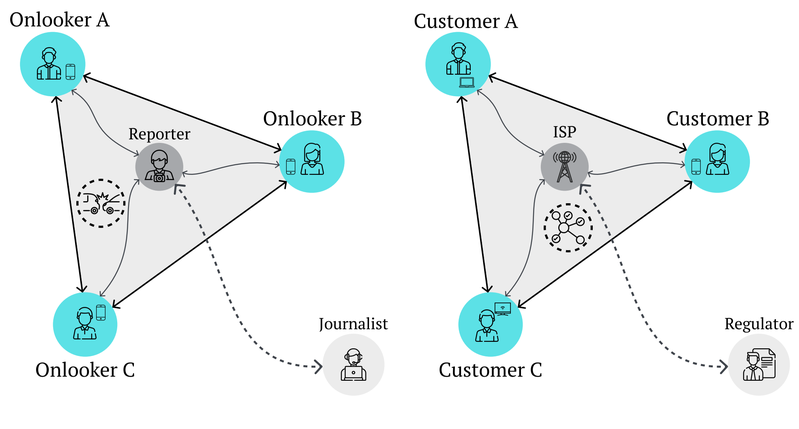
2. Permissionless Consensus

In the context of fully decentralized and trustless environments, achieving **time synchronization** can be transposed to the general problem of achieving permissionless consensus, fulfilling the need for **ordering and synchronizing** events at the same pace, in an environment where the participants are **not necessarily trusted**.

Permissionless consensus with a Turing Complete environment enables the decentralized execution of location-based **smart contracts**.



3. Verifiable Proof-of-Location



With the witnesses agreeing on a location, short-range communication, and internal clock synchronization, the zone is ready to generate **correct** and **spatio-temporally sound** location proofs, achieving decentralized, privacy preserving, verifiable, and secure Proof-of-Location.

The verification process can be automated by any verifier that has access to the entities' public keys and the Proof-of-Location certificate, just like any typical **digital signature verification**, integrated with digital applications of all kinds.