A coauthority is made up of servers that dynamically form a tree. This makes everything scalable.

The DeDiS team is working on a number of projects related to coauthorities, or large-scale collective authorities, that distribute trust among a number of independent parties.

By decentralising trust, we go from weakest-link to strongest-link security.

With no single trusted party, coauthorities can:

- enable software developers to collectively sign updates
- provide public randomness
- enable privacy-conscious medical-data sharing
- prove that a document existed at a given time

Many other protocols can be based on coauthorities, e.g.:

**CoSi**

Enabling a large number of witnesses to sign off a given message or to reject it. This is done using the Collective Signing (CoSi) protocol. It is much faster than other protocols (JVSS and naive) for large numbers of signers.

**PriFi**

Privacy-Preserving Wi-Fi (PriFi) enables anonymous communication with strong guarantees of anonymity:
- is built upon communication trees provided by CoSi
- uses decentralized authorities
- relies on Chaum’s well-known Dining Cryptographers
- provides theoretically-strong anonymity

The main challenges are scalability and efficiency, both partly solved by tailoring the system for wireless networks.

**ByzCoin**

A novel consensus algorithm for Bitcoin, which can be deployed to any blockchain-based system:
- increases Bitcoin’s core security guarantees
- is based on PBFT, but preserves decentralization
- uses tree-based communication and collective signing to enable high scalability with low latency of transactions
- achieves throughput comparable to VISA’s average throughput (2000 tps)

Our Secure Distributed API (SDA) enables different protocols to live in a coauthority structure. Nodes work together as needed, then dissolve again. Easy-to-use structures for testing and simulating new protocols, ranging from single-node testing to simulating 32,000 nodes.

https://github.com/dedis/coauthority