AXA Research Program in Information Security and Privacy

Researching decentralized systems to guarantee security, availability and privacy on the web.

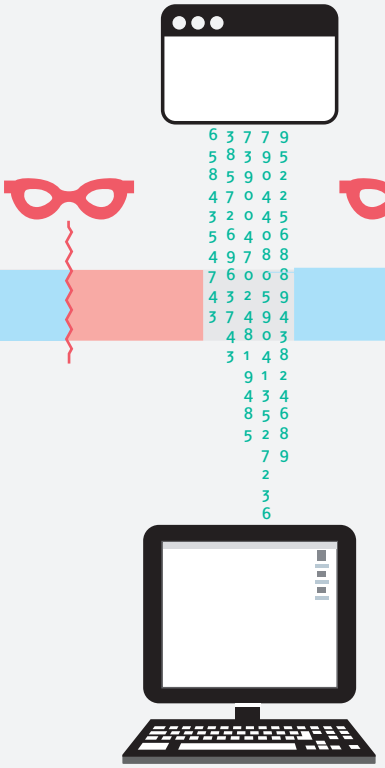
Internet security often relies on centralized unique authorities which are not always trustworthy.

Using a scalable decentralized network of independent servers to form a collective authority (cothority) allows the trust to be distributed among many entities thus making the system inherently more secure.

Centralized authorities

Single point of failure

Not always trustworthy



Decentralized authorities

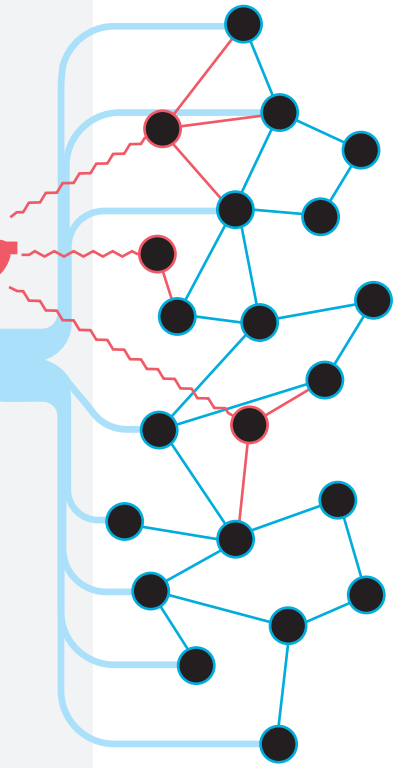
cothorities

Decentralized trust

Strongest-link security

Increased availability

Scalability



Multiple uses (protocols)

CoSi

collective signing

Provides transparency by enabling many witnesses to cosign authoritative statements.

PriFi

Privacy-Preserving Wi-Fi

Enables communication with strong guarantee of anonymity between the nodes in the network.

Byzcoin

A scalable and low latency consensus algorithm for Blockchains using tree-based communication.

AXA Research Fund
Through Research, Protection

EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE