Programme de recherche AXA en sécurité de l'information et confidentialité des données

Recherche sur des systèmes décentralisés pour garantir la sécurité, la disponibilité et la confidentialité sur internet.

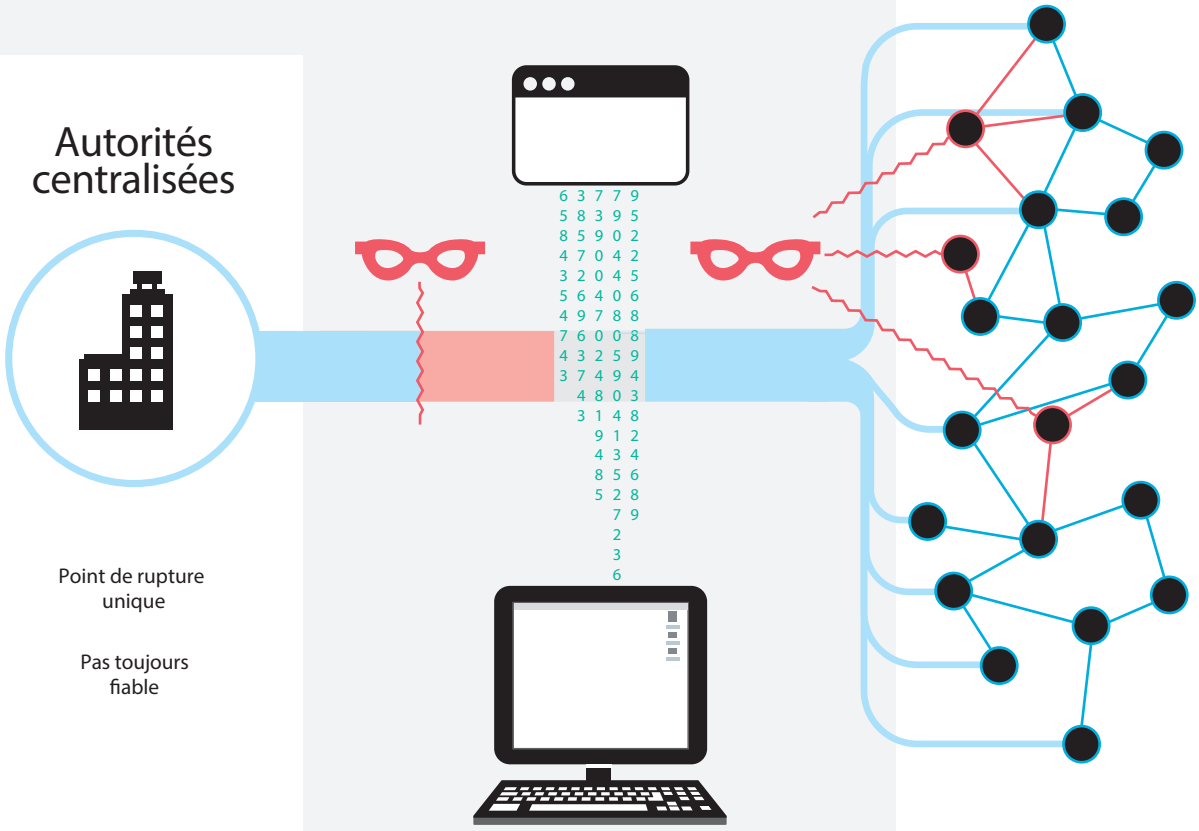
La sécurité d'internet repose souvent sur des autorités uniques et centralisées, lesquelles ne sont pas toujours fiables.

Afin de rendre le système plus sûr, on peut utiliser un système multi-échelle décentralisé de serveurs, qui forment une autorité collective (co-autorité) qui distribuent les contrôles sur plusieurs entités.

Autorités centralisées

Point de rupture unique

Pas toujours fiable



Autorités décentralisées
co-autorités

Contrôles décentralisés

Sécurité du maillon fort

Disponibilité accrue

Déployable sur de multiples échelles

De nombreuses applications (protocoles)

CoSi
signatures collectives

Transparence: on permet à de multiples témoins de co-signer des déclarations officielles.

PriFi
wifi confidentiel

Permet des communications avec forte garantie d'anonymat entre les nœuds du réseau.

ByzCoin

Un algorithme de consensus multi-échelle à basse latence pour chaînes de blocs utilisant des communications en arborescence.

Fonds AXA pour la Recherche
Chercher pour protéger
EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE