

Building the decentralized web

Carl Youngblood



Blockchain Speaker and Advisor





INFORMATION SECURITY

[Questions](#) [Tags](#) [Users](#) [Badges](#) [Unanswered](#) [Ask Question](#)

What steps remain for a robust, neutral and surveillance-proof Internet? [closed]

Will we ever get to a point where the core protocols are robust and secure enough that surveillance and centralized control of the Internet becomes effectively infeasible?

or the public consciousness as we strive to determine best practices in governance for the internet era. People are also concerned about network neutrality and how the Internet currently relies on protocols (such as DNS) that require regulation by central authorities, which increases the potential for abuse by oppressive and corrupt regimes.

My question is: what efforts are currently underway to develop alternative secure distributed protocols that do not rely on central authorities? Which initiatives are the most mature? What critical pieces of infrastructure are still missing? What projects would be good to contribute to in this regard? Will we ever get to a point where the core protocols are robust and secure enough that surveillance and centralized control of the Internet becomes effectively infeasible?

[privacy](#) [protocols](#) [surveillance](#)

[share](#) [edit](#) [delete](#) [flag](#)

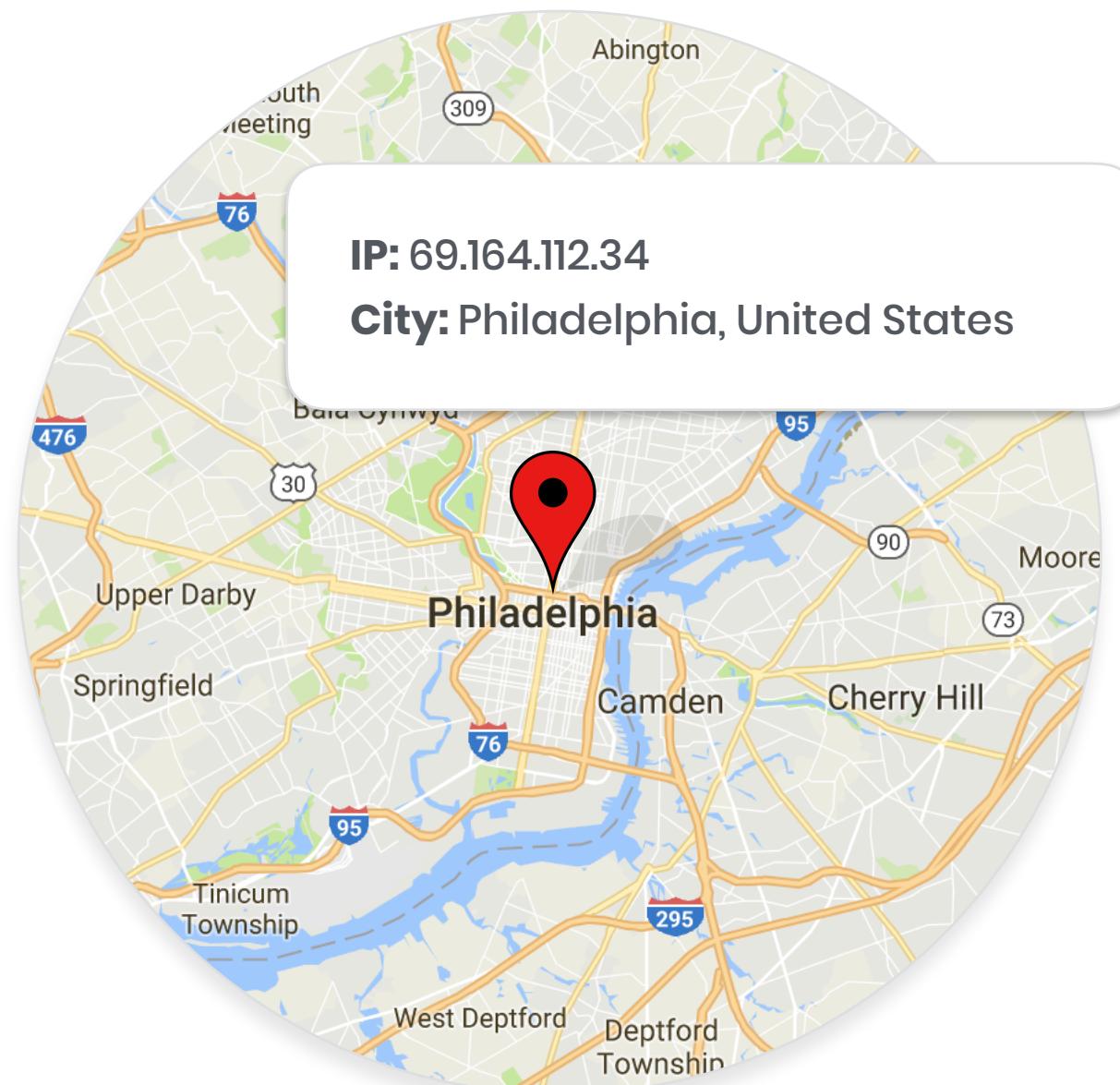
asked Jan 9 '14 at 10:29

 **cayblood**
114 ⚡ 2

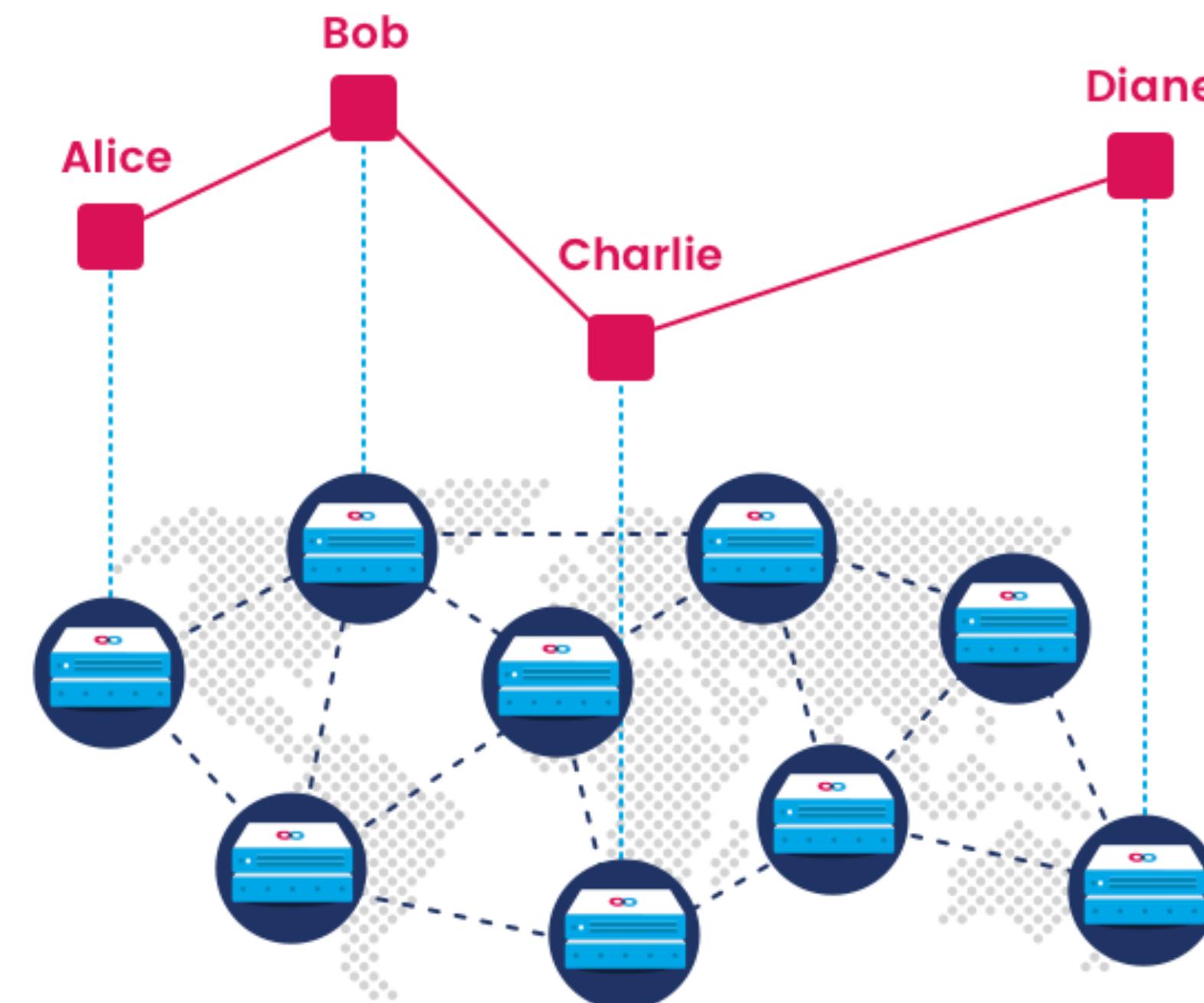
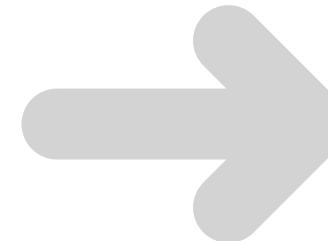
The long hard road to decentralization



web2 vs web3 Addressing



IP addresses are
geolocatable



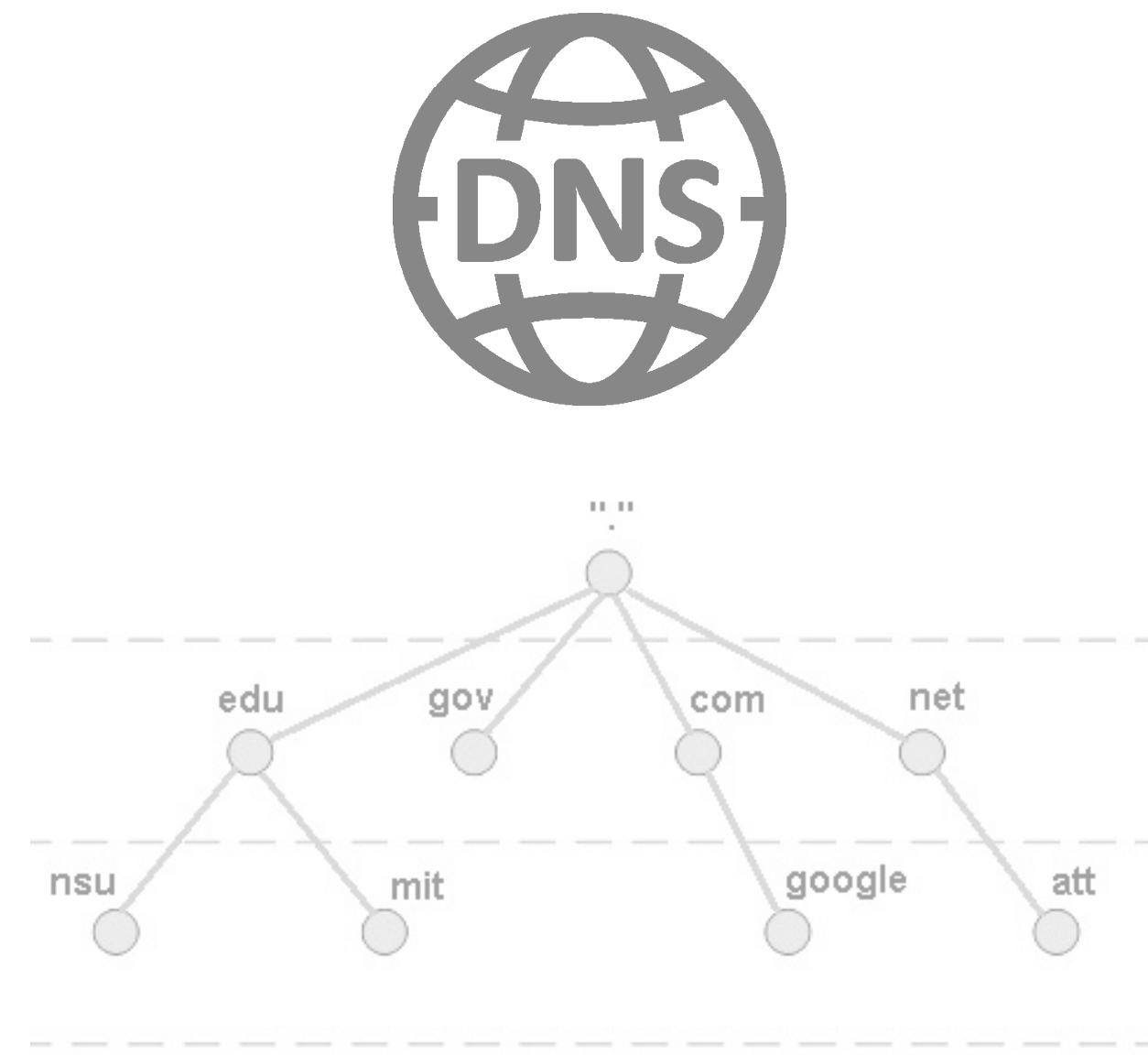
Web3 addresses don't match
physical topology

Peer-to-peer overlay

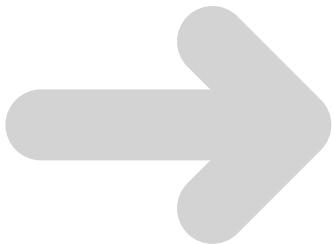
Physical network

web2 vs web3

Name services



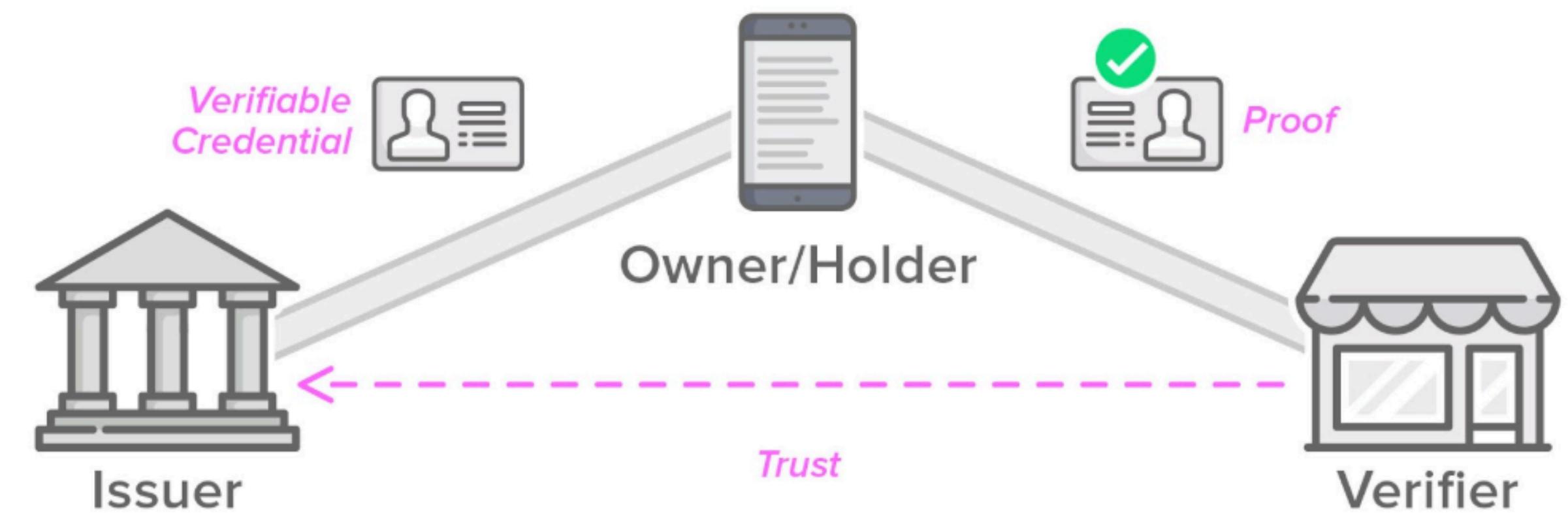
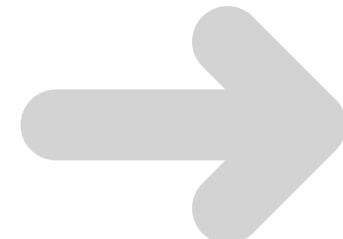
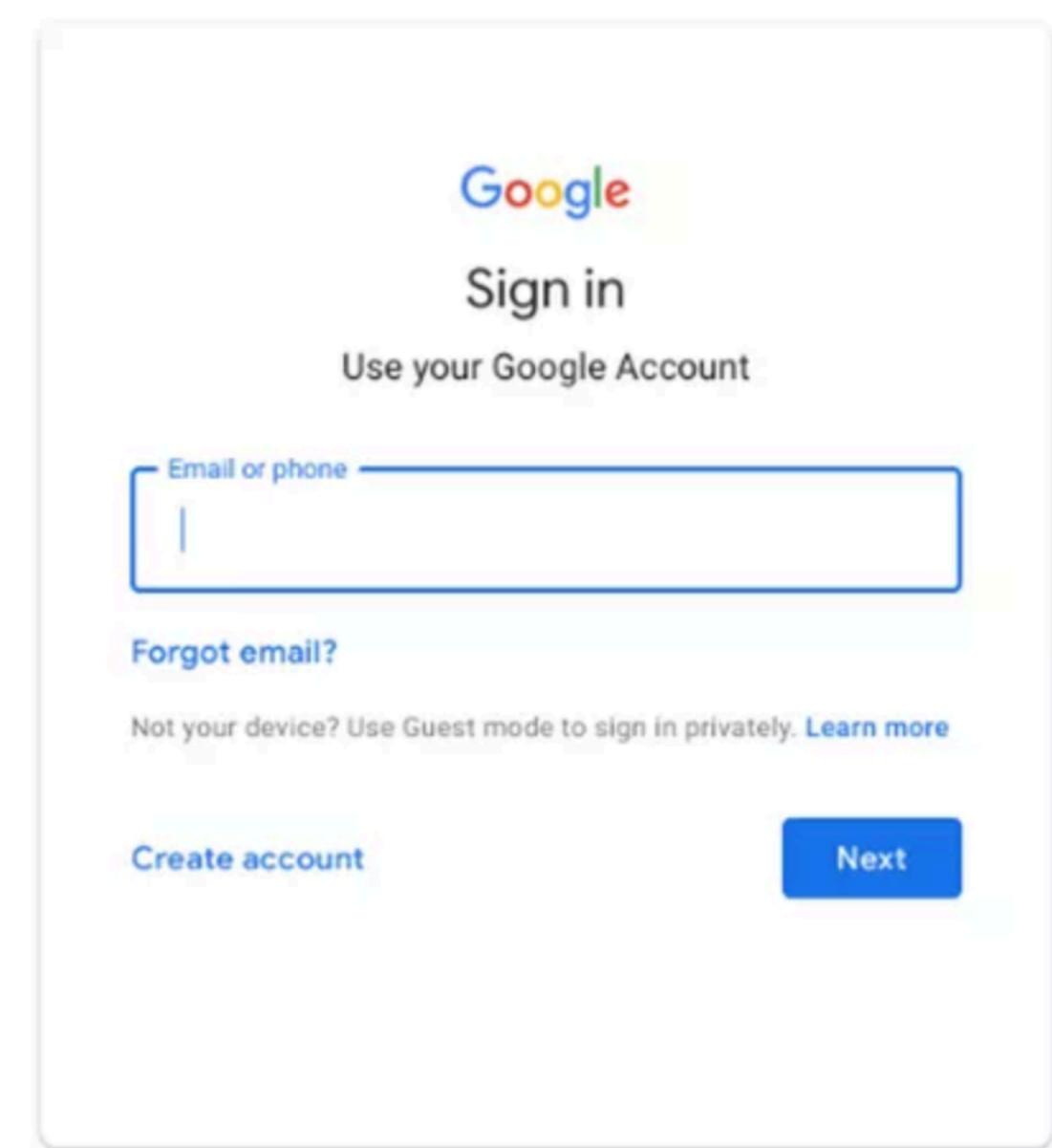
Hierarchical



Managed on
blockchain



web2 vs web3 Identity



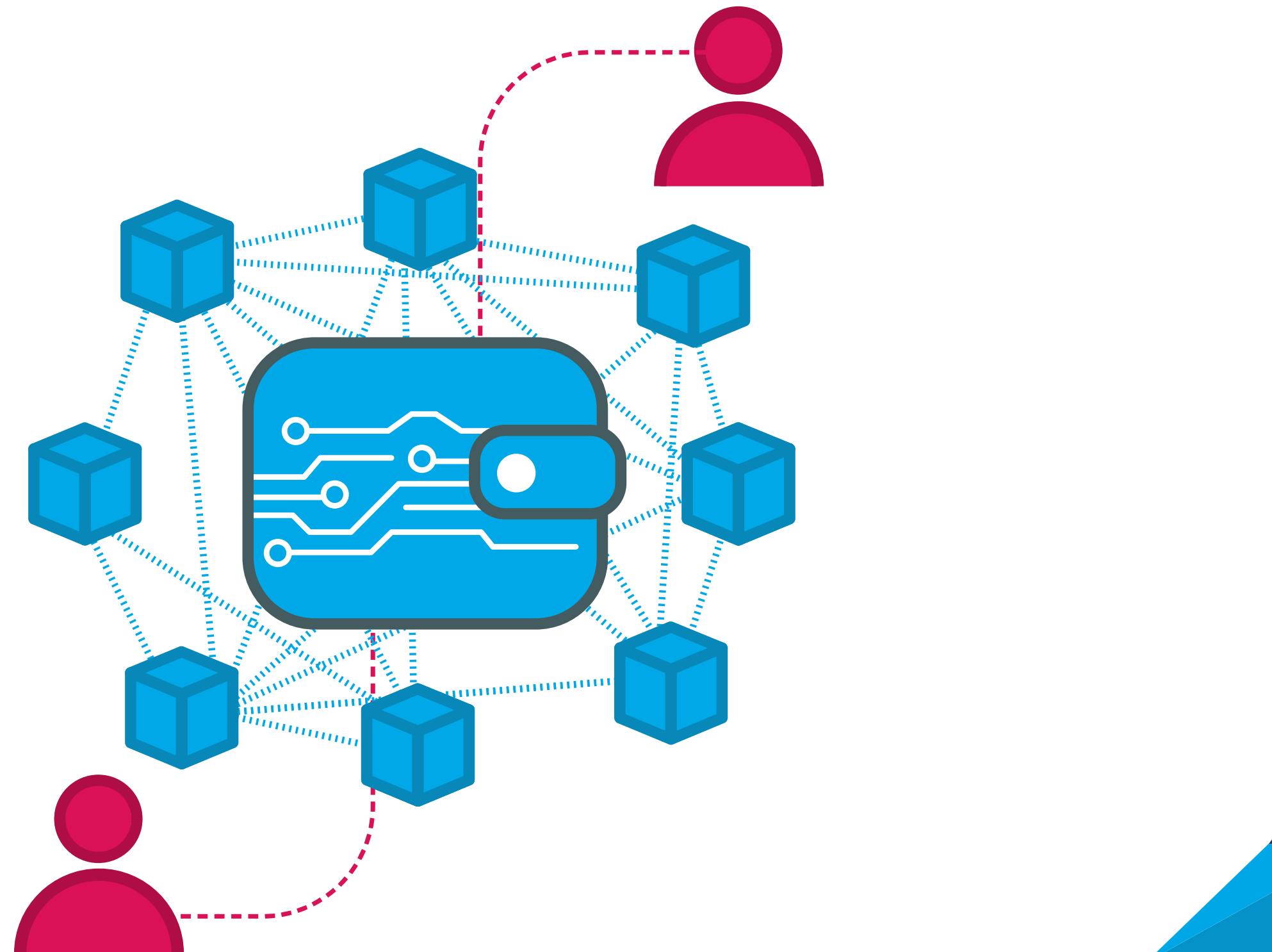
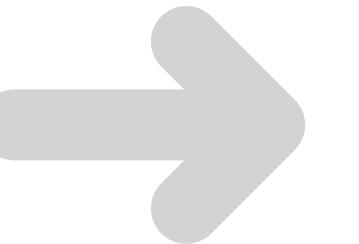
Federated authentication systems -
thousands of passwords

Self-sovereign identity

web2 vs web3 Payments



centralized payment
systems



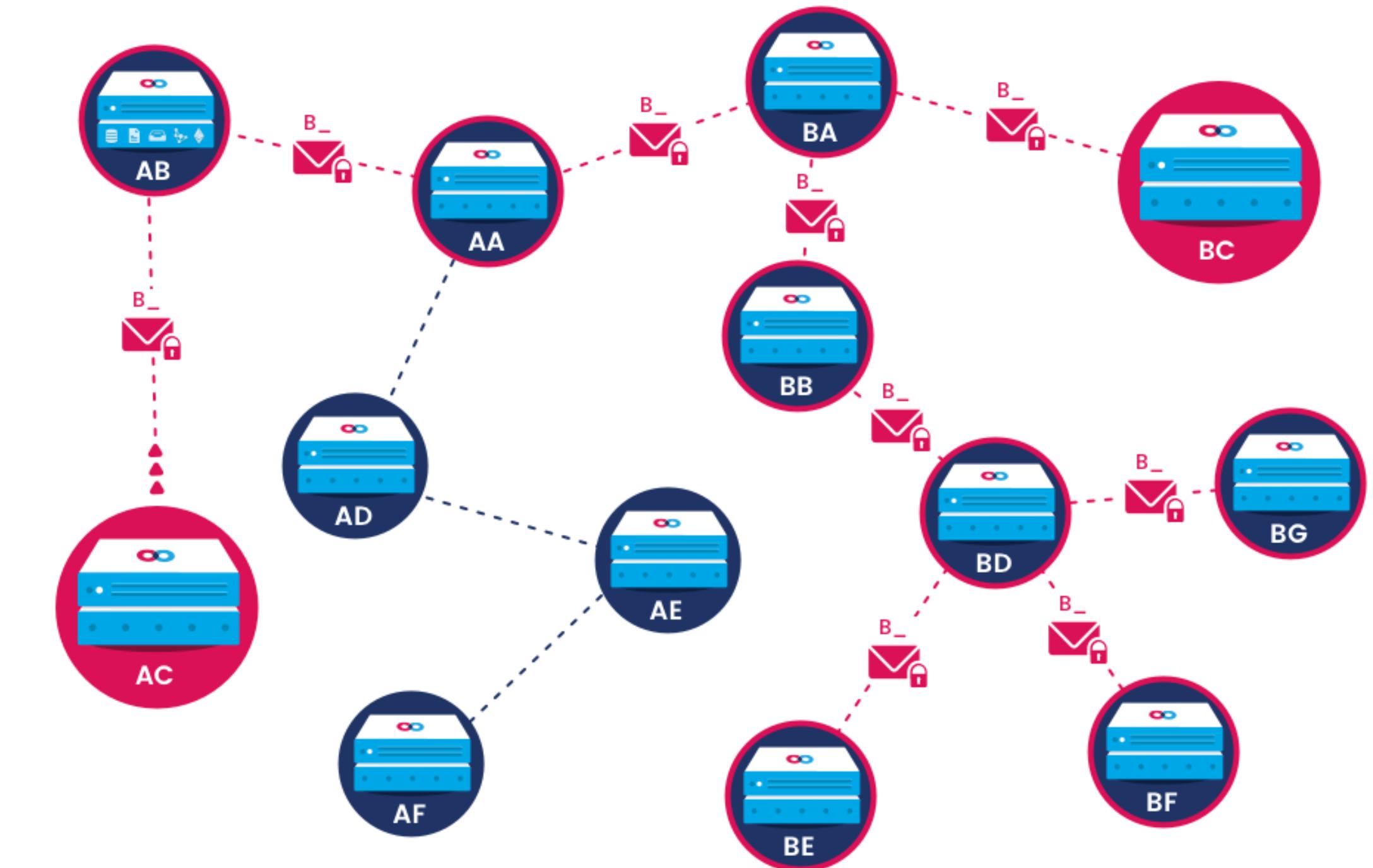
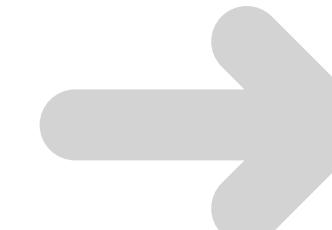
cryptocurrencies

web2 vs web3

Communications

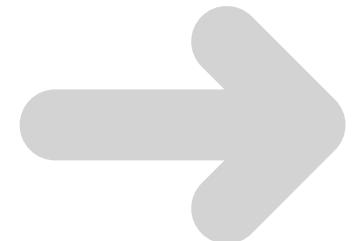
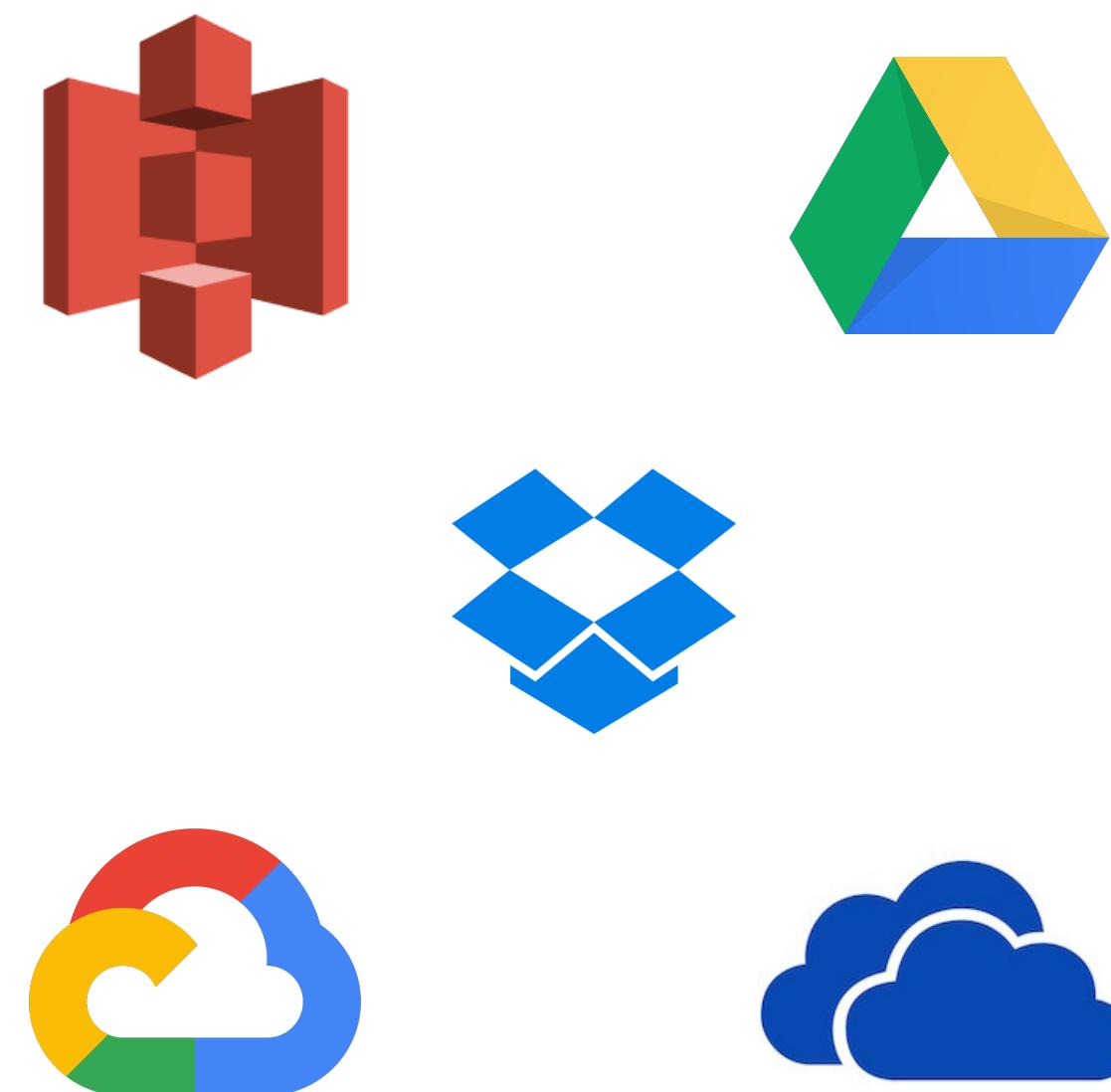


centralized, siloed

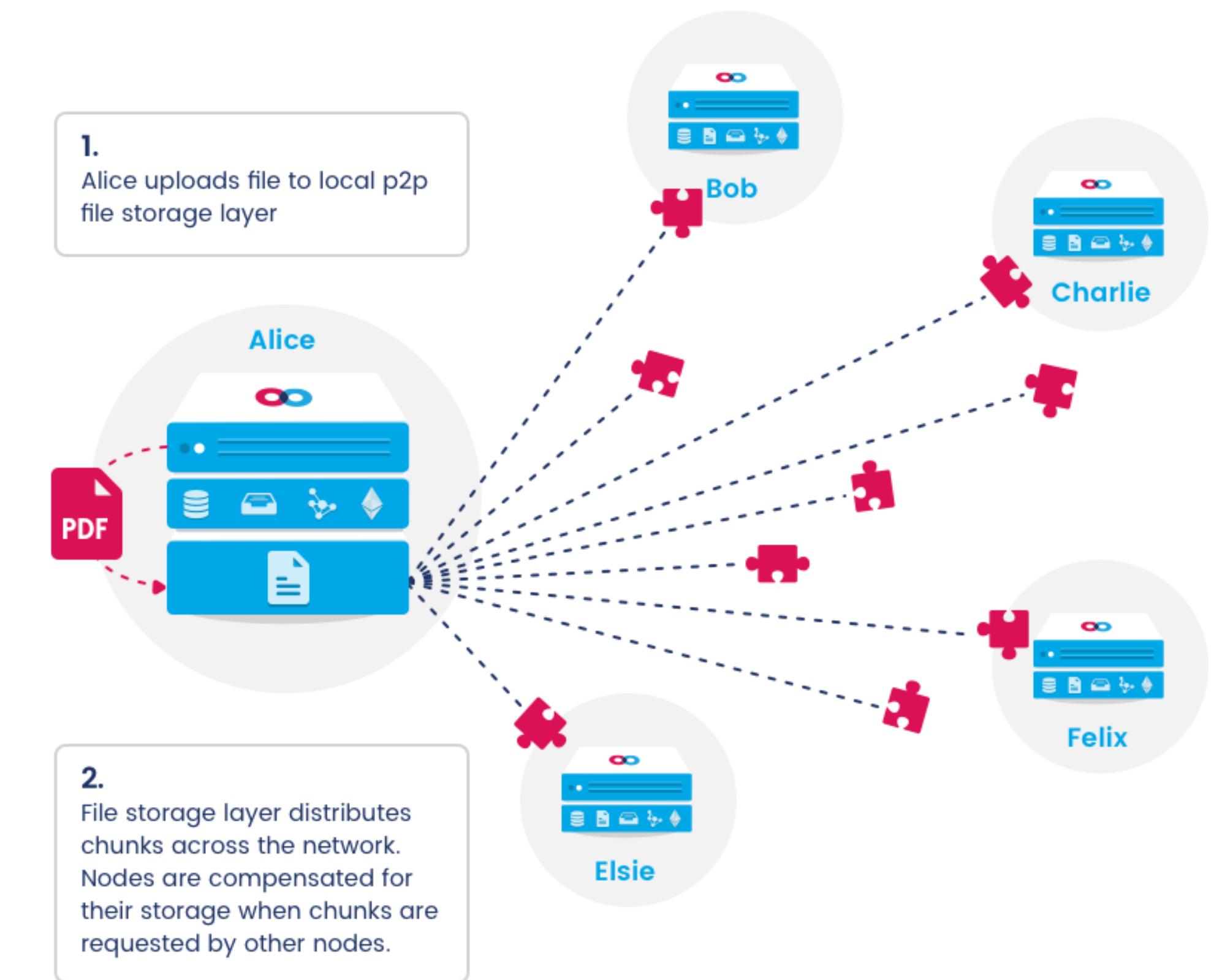


peer-to-peer
surveillance-resistant
censorship-resistant

web2 vs web3 File storage



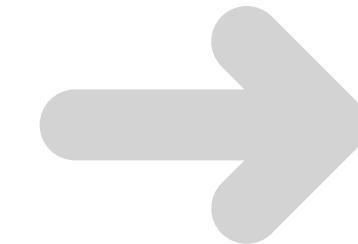
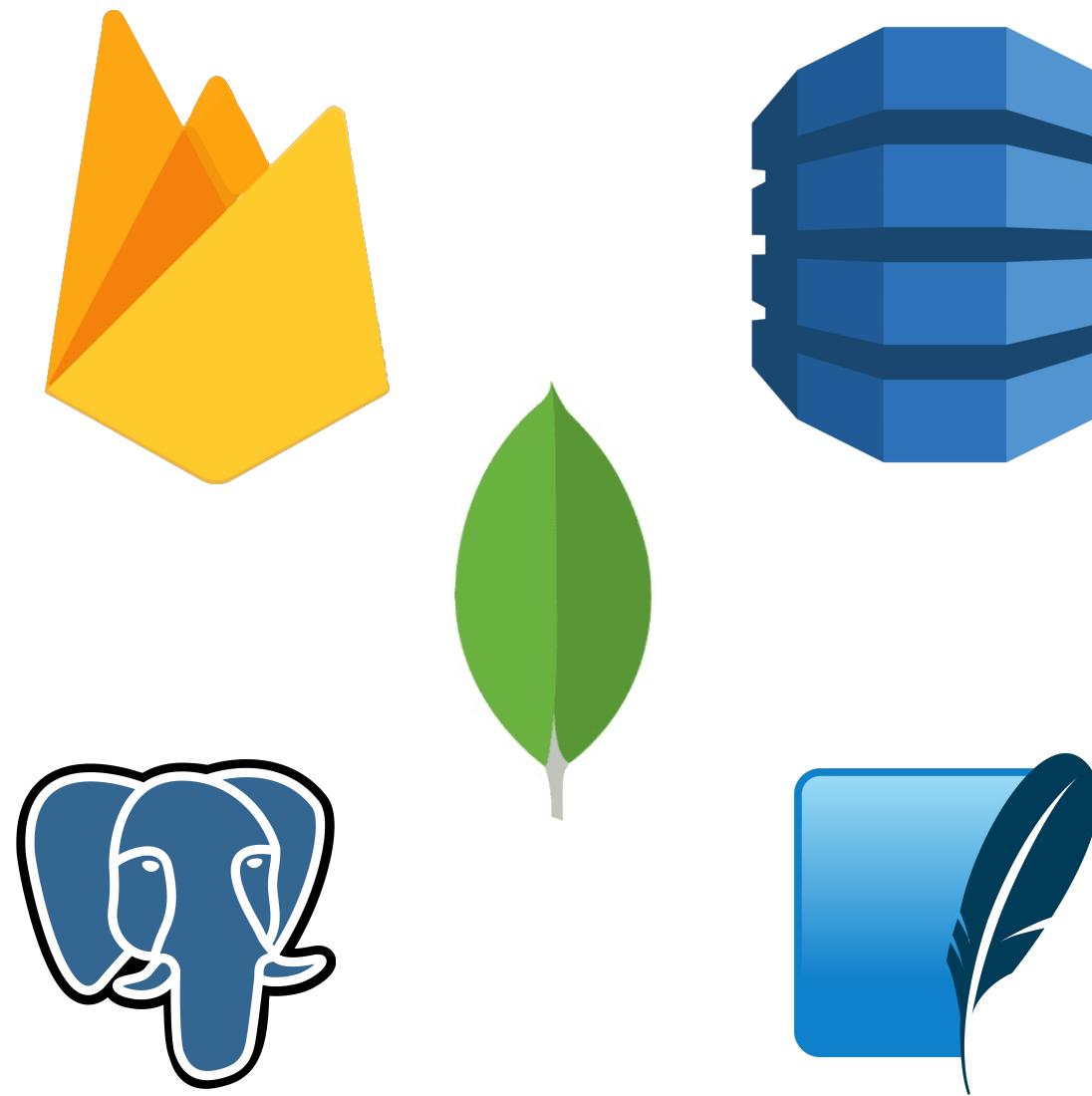
data is stored on infrastructure
managed by centralized providers



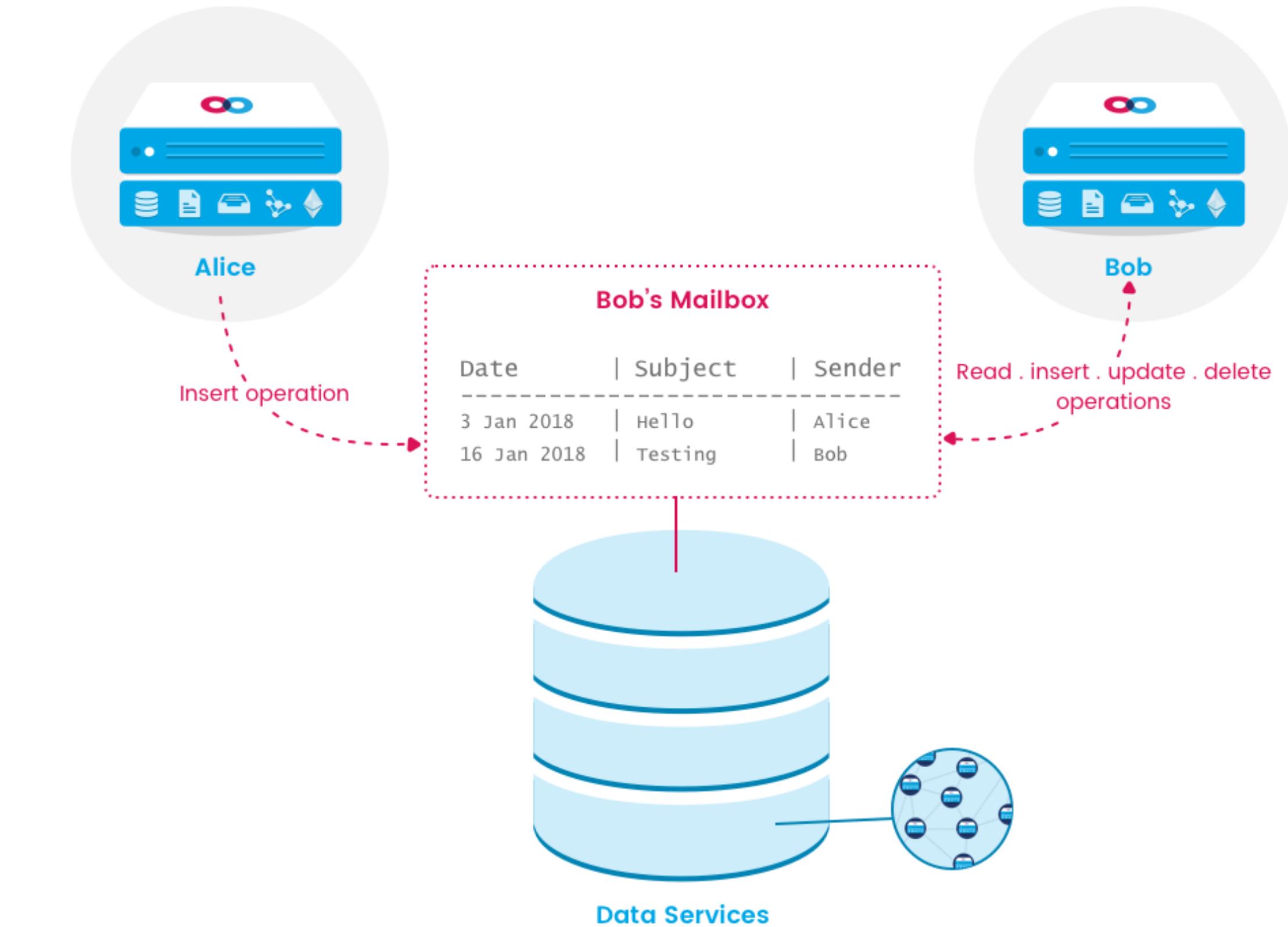
data is stored redundantly on
independent peers

web2 vs web3

Data services



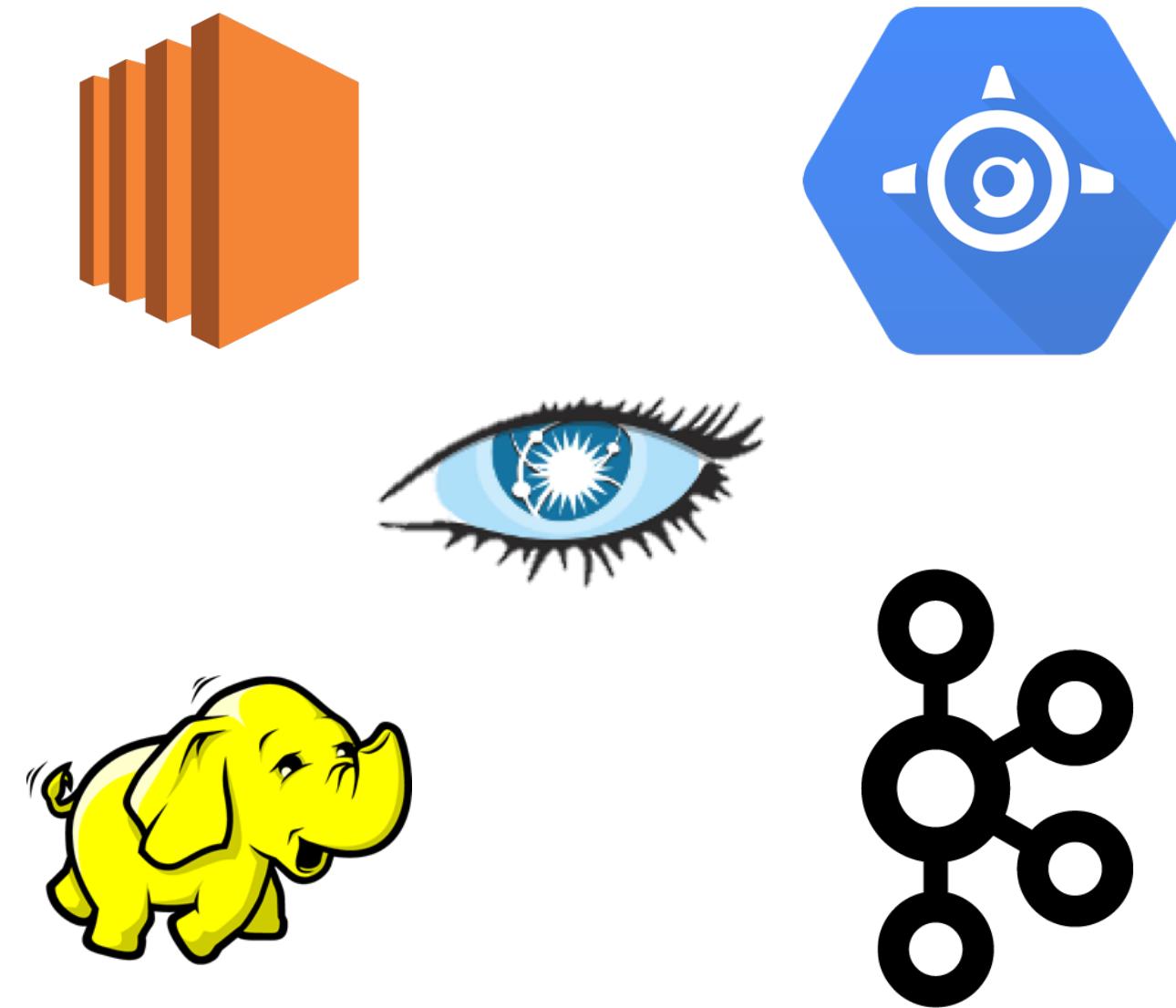
data is stored on infrastructure
managed by centralized providers



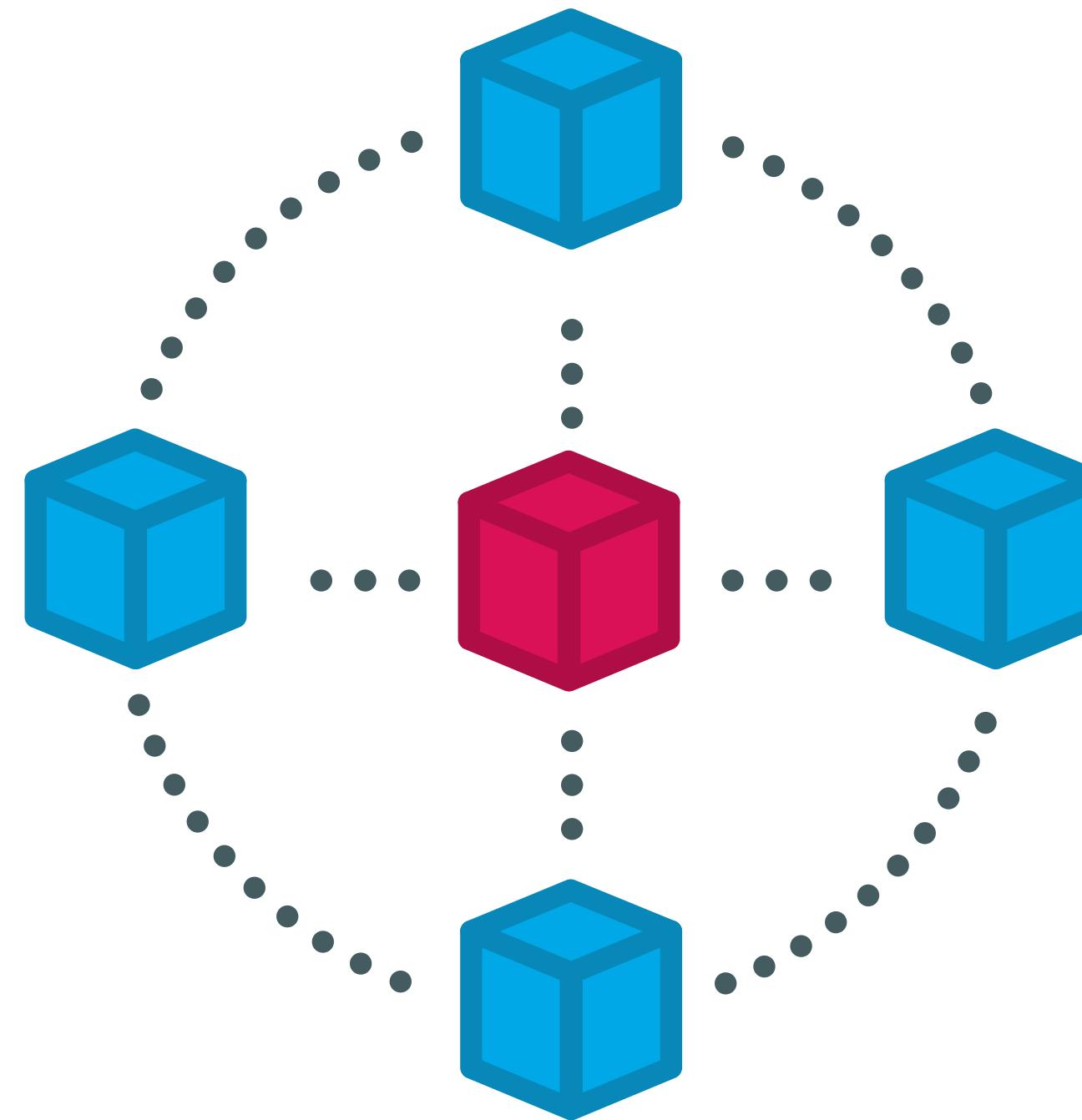
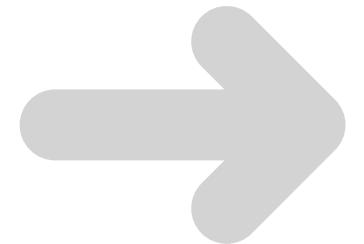
data is stored redundantly on a
cluster of independent peers

web2 vs web3

Computing services



jobs are processed on
managed infrastructure



jobs are executed by
independent peers

web2 vs web3

Incentivization



web2 vs web3

Incentivization

A token must work as a **necessary element** of a **self-sustaining** system which is a **public utility**.



from Mike Goldin's Cryptosystems Manifesto

web2 vs web3

Incentivization

- A token must work as a **necessary element** of a **self-sustaining** system which is a **public utility**.
- A token is a **necessary element** of a system if the use of anything else in its place would damage the system's normal functioning.



from Mike Goldin's Cryptosystems Manifesto

web2 vs web3

Incentivization

- A token must work as a **necessary element** of a **self-sustaining** system which is a **public utility**.
- A token is a **necessary element** of a system if the use of anything else in its place would damage the system's normal functioning.
- A system is **self-sustaining** *if it would continue to function normally in the indefinite absence of its creators.*



from Mike Goldin's *Cryptosystems Manifesto*

web2 vs web3

Incentivization

- A token must work as a **necessary element** of a **self-sustaining** system which is a **public utility**.
- A token is a **necessary element** of a system if the use of anything else in its place would damage the system's normal functioning.
- A system is **self-sustaining** *if it would continue to function normally in the indefinite absence of its creators.*
- A system is a **public utility** if it is permissionless, rent-free, and does something useful.

from Mike Goldin's Cryptosystems Manifesto



web2 vs web3

Incentivization (is hard)

“You can design incentives of your choosing, by giving them block rewards. Put another way: you can get people to do stuff, by rewarding them with tokens. Blockchains are incentive machines.”



Trent McConaghy: “Can Blockchains Go Rogue?”

web2 vs web3

Incentivization (is hard)

“I see this as a superpower. The block rewards function defines what you want network participants to do. Then the question is: what do you want people in your network to do? It has a crucial corollary: how well can you communicate that intent to the machines? This is a devilish detail. Do we really know how to design incentives?”



Trent McConaghy: “Can Blockchains Go Rogue?”

web2 vs web3

Incentivization (is hard)

“In summary: good incentive systems are notoriously difficult to create under the best of circumstances. Under Blockchain systems—where code is law, etched in stone, and deployed to a wide community of pseudonymous stakeholders—good incentive systems are all the harder to get right. The success of Bitcoin should not make us complacent and optimistic: our incentive design paradigms needs to be scrupulous, slow growing, with a framework of checks and balances.”

Elad Verbin: “Behavioral Crypto-Economics”





“The idea that you can create verifiably scarce digital assets is certainly novel and represents a breakthrough in our history. But I actually think that another potentially more powerful development is getting little attention: the ability to remake the big businesses that we know today as networks that are decentralized, peer-to-peer, and user-owned.”

*Laura Shin
Episode 83
Unchained Podcast*