What is Bitcoin?

Bitcoin - is a payment ~~system/currency/network~~ **PROTOCOL** invented by Satoshi Nakamoto,who published the invention in 2008 and released it as open-source software in 2009. The system is peer-to-peer; users can transact directly without needing an intermediary. Transactions are verified by network nodes and recorded in a public distributed ledger called the block chain.

Byzantine generals problem.

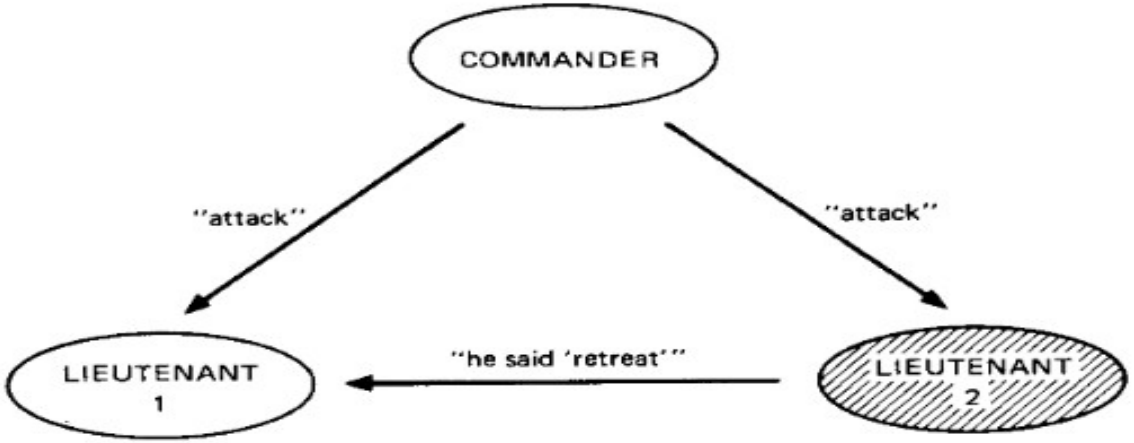


Fig. 1. Lieutenant 2 a traitor.

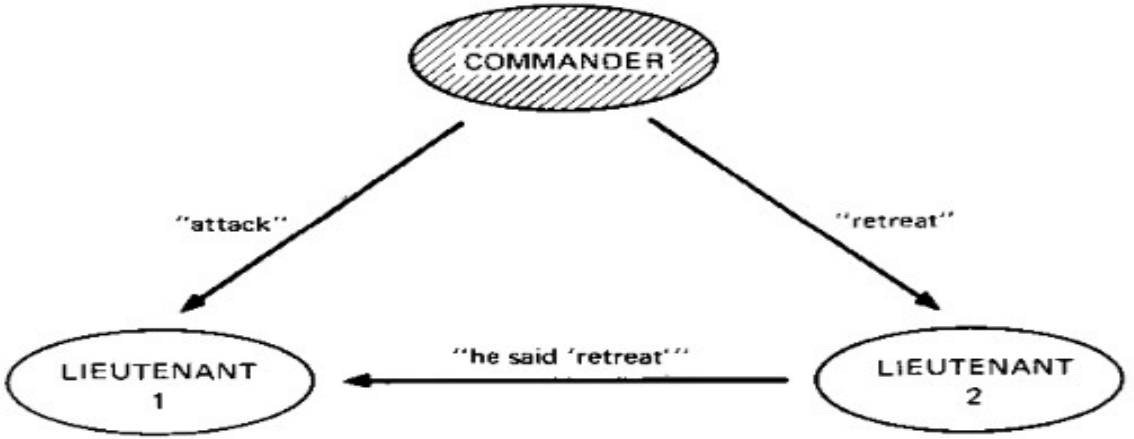
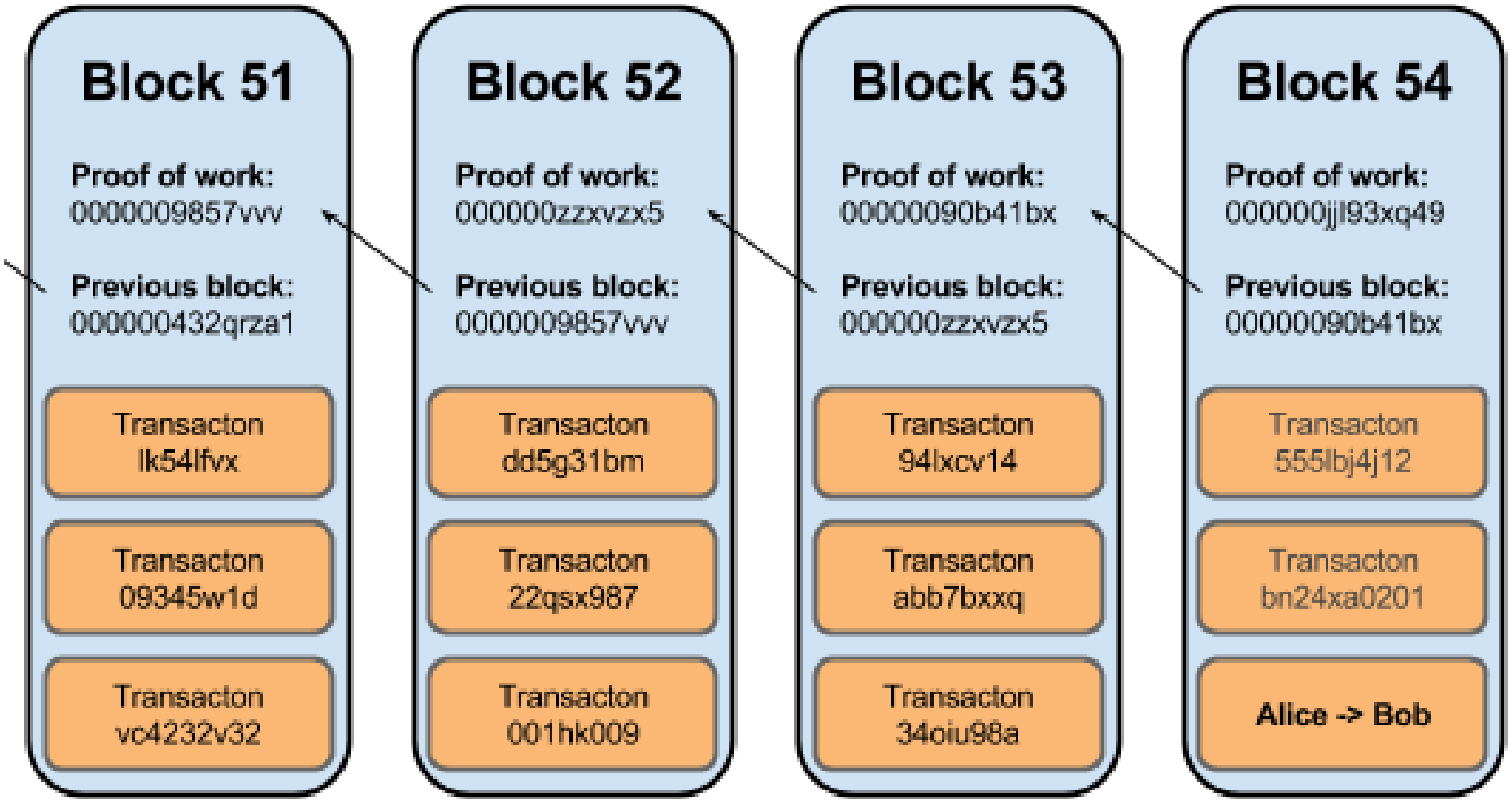
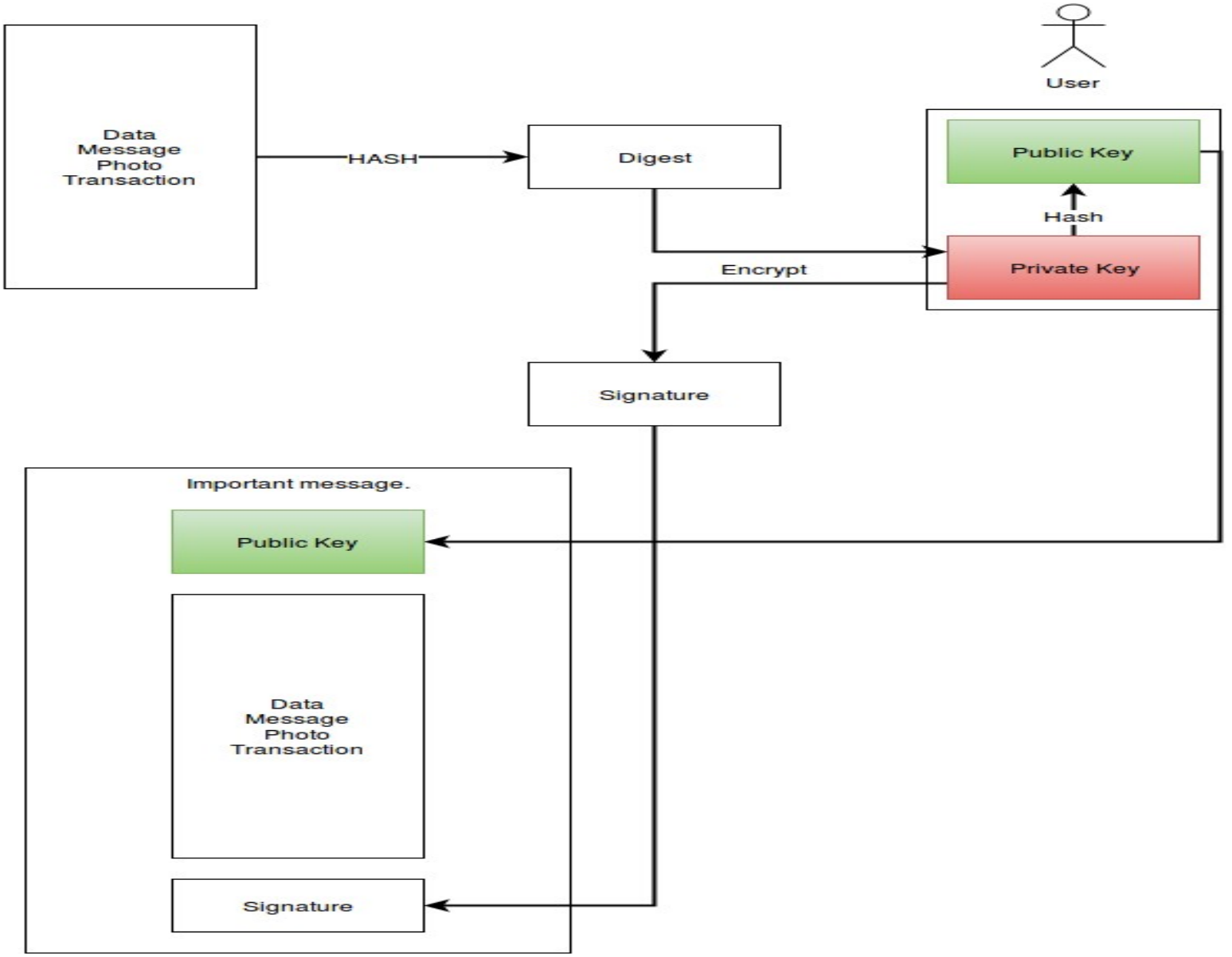


Fig. 2. The commander a traitor.

Blockchain=Solution



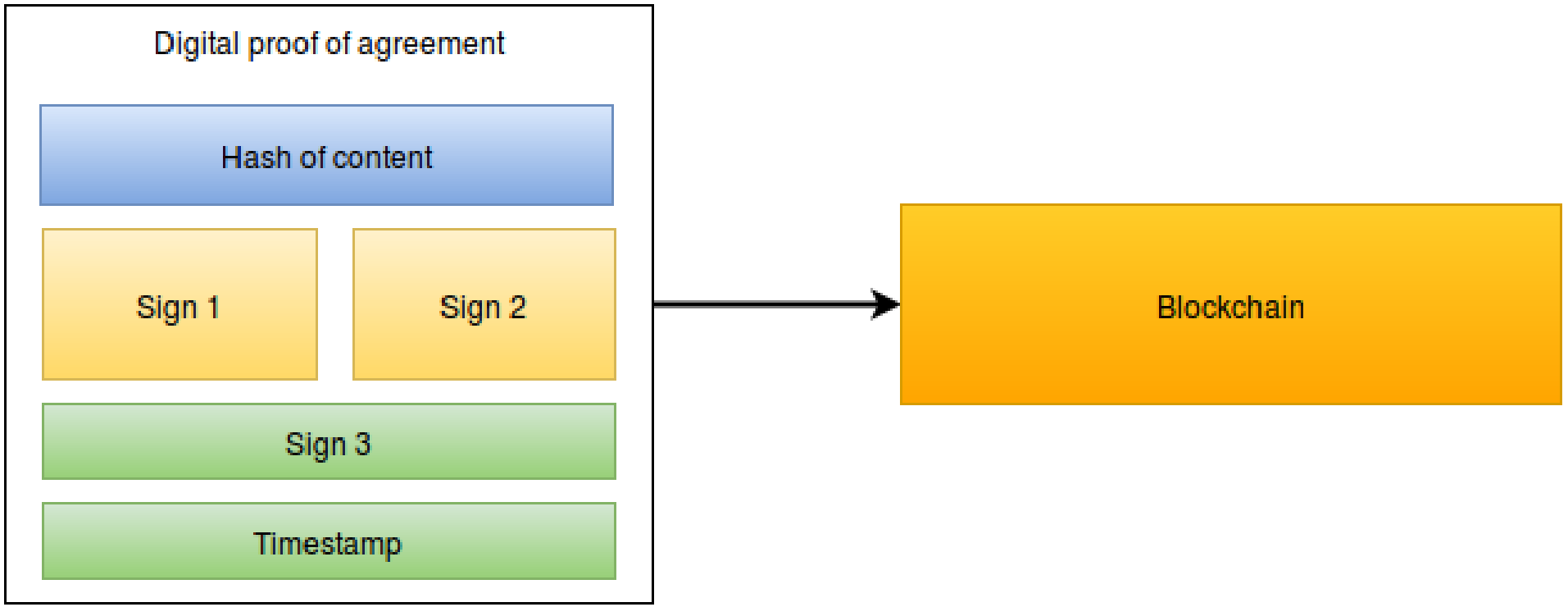
Transaction sign



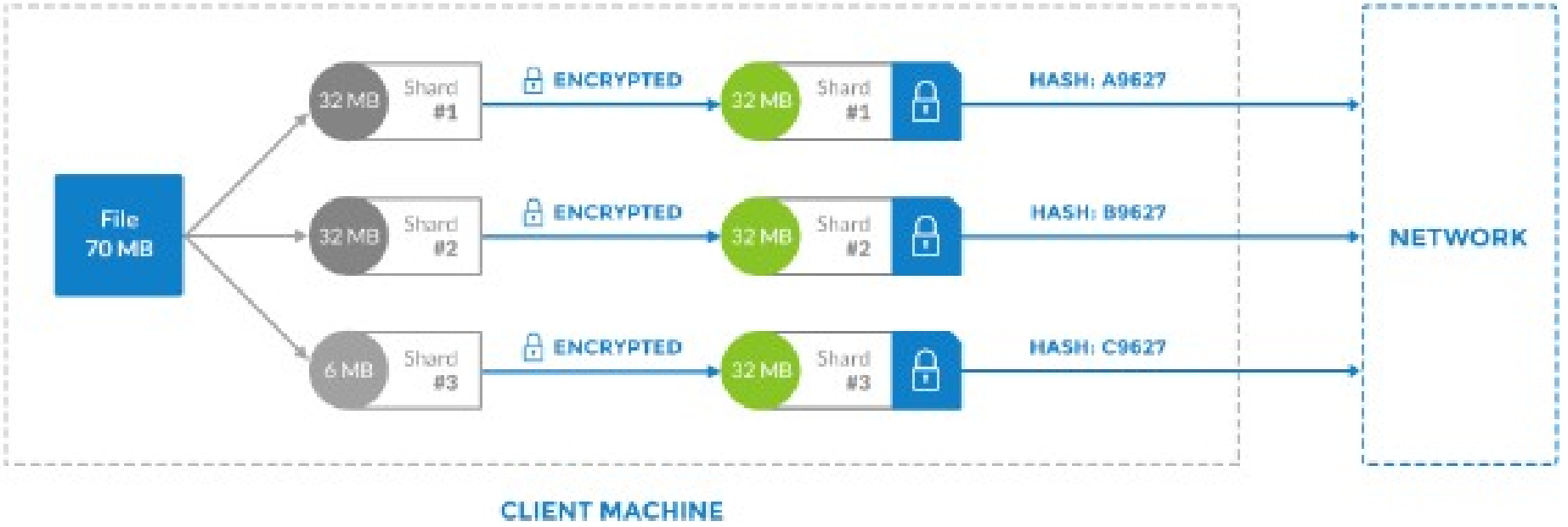
Possible aplications

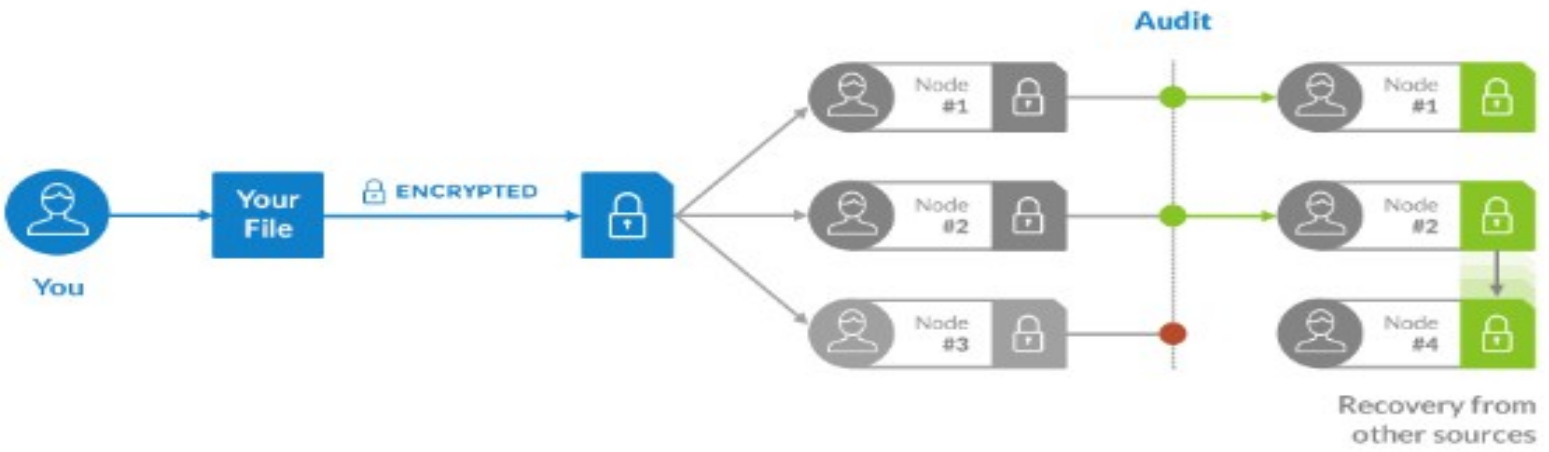
- Smart contracts
- Digital documents notarization (Ethereum)
- Funds transfer
- Sending Messages (bitmessage)

Digital document notarization



Distributed data cloud.

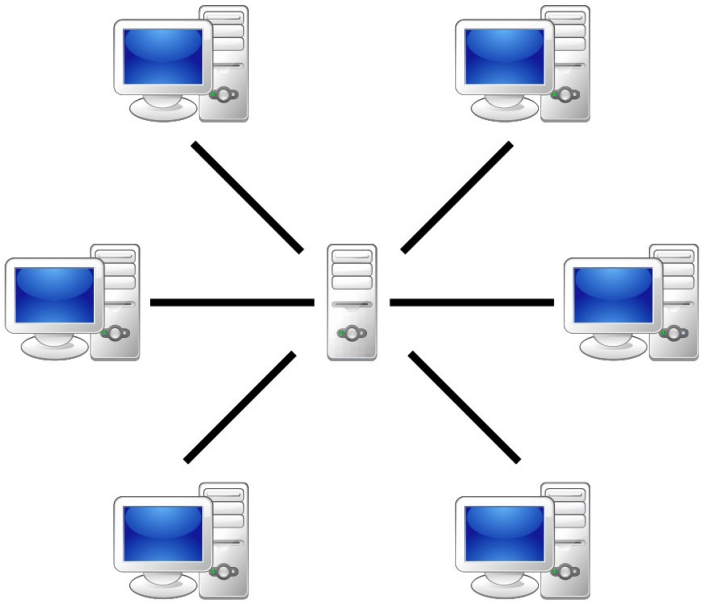




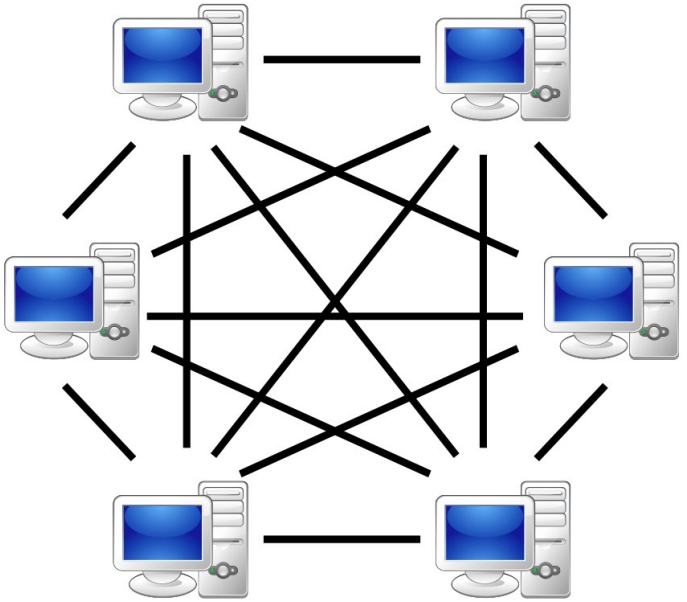
Infrastructure

- 17.6 petaflops: Computing power of Titan, the world's top supercomputer
- 162 petaflops: Combined computing power of all 500 of the world's most powerful supercomputers
- 1,085 petaflops: Computing power need to equal bitcoin network hashrate

Infrastructure



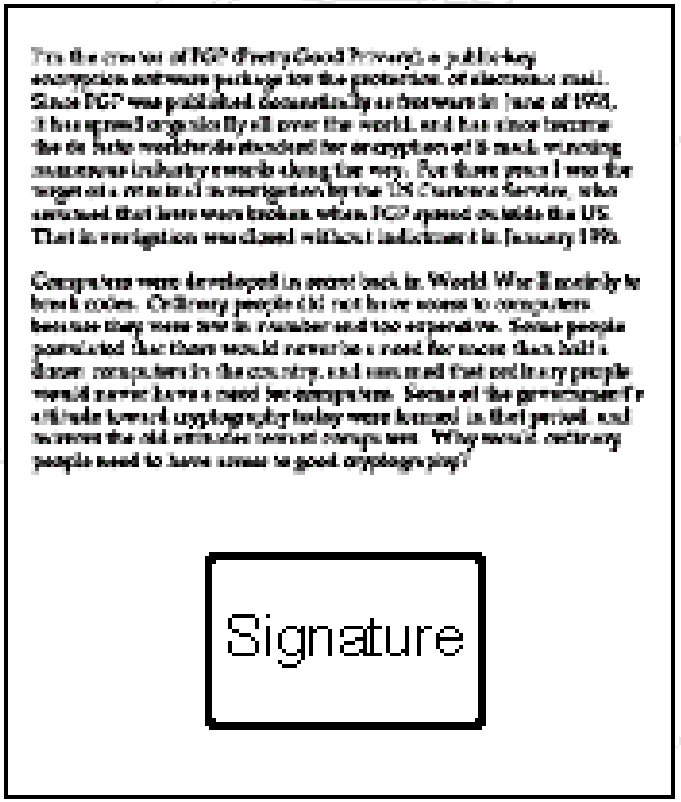
Server-based



P2P-network

Sign methods

Offline verification



Signature

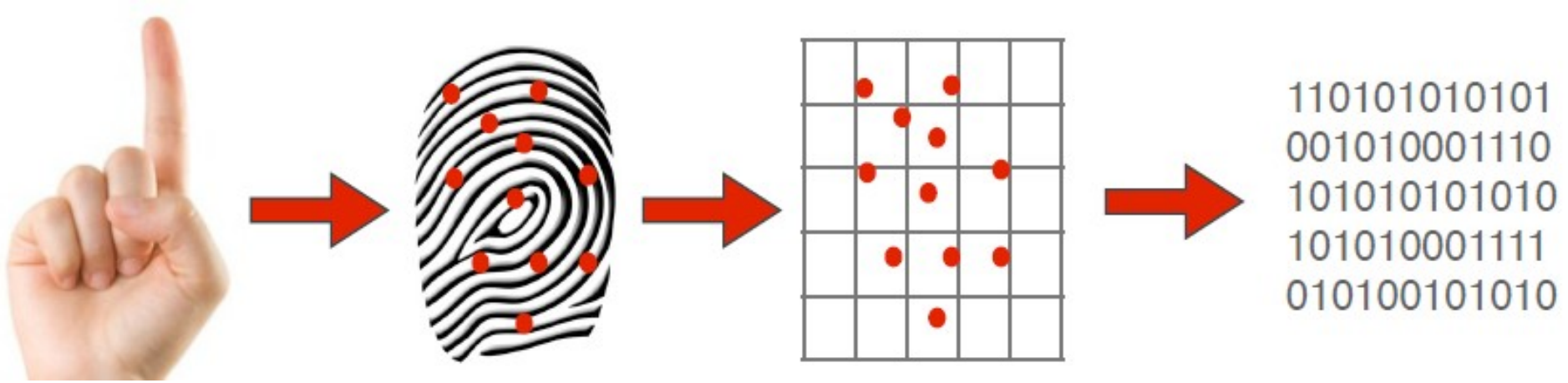
Hash

Message Digest

Decrypt with Public Key

Message Digest

What about biometry?



Pros of Blockchain based technologies and applications

- Cost efficient
- Distibuted network
- Offline verification
- Highly redundant
- Open specification
- Strong cryptography
- Scalability

Q&A