

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.

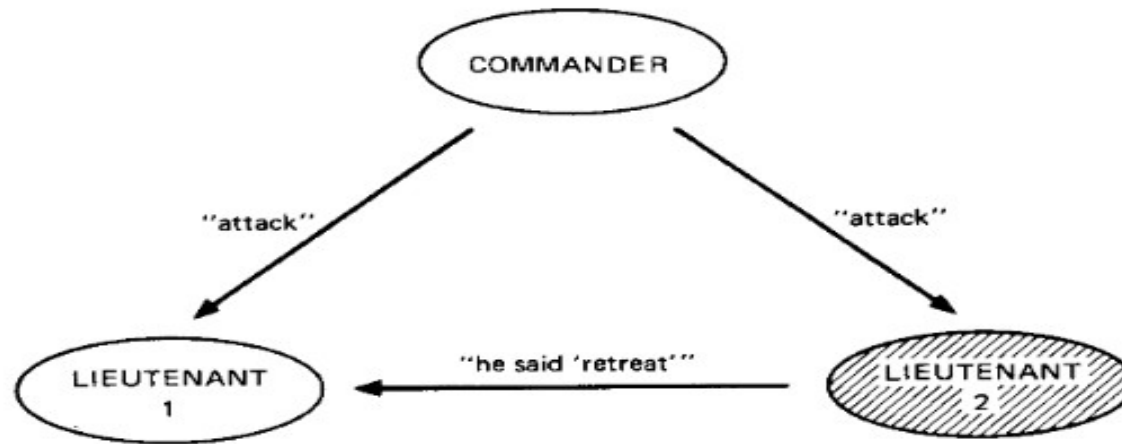


Fig. 1. Lieutenant 2 a traitor.

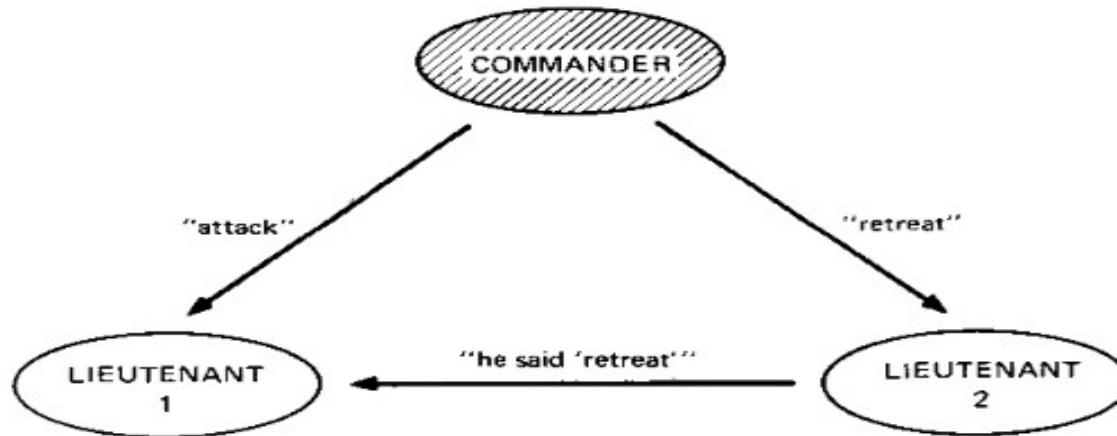
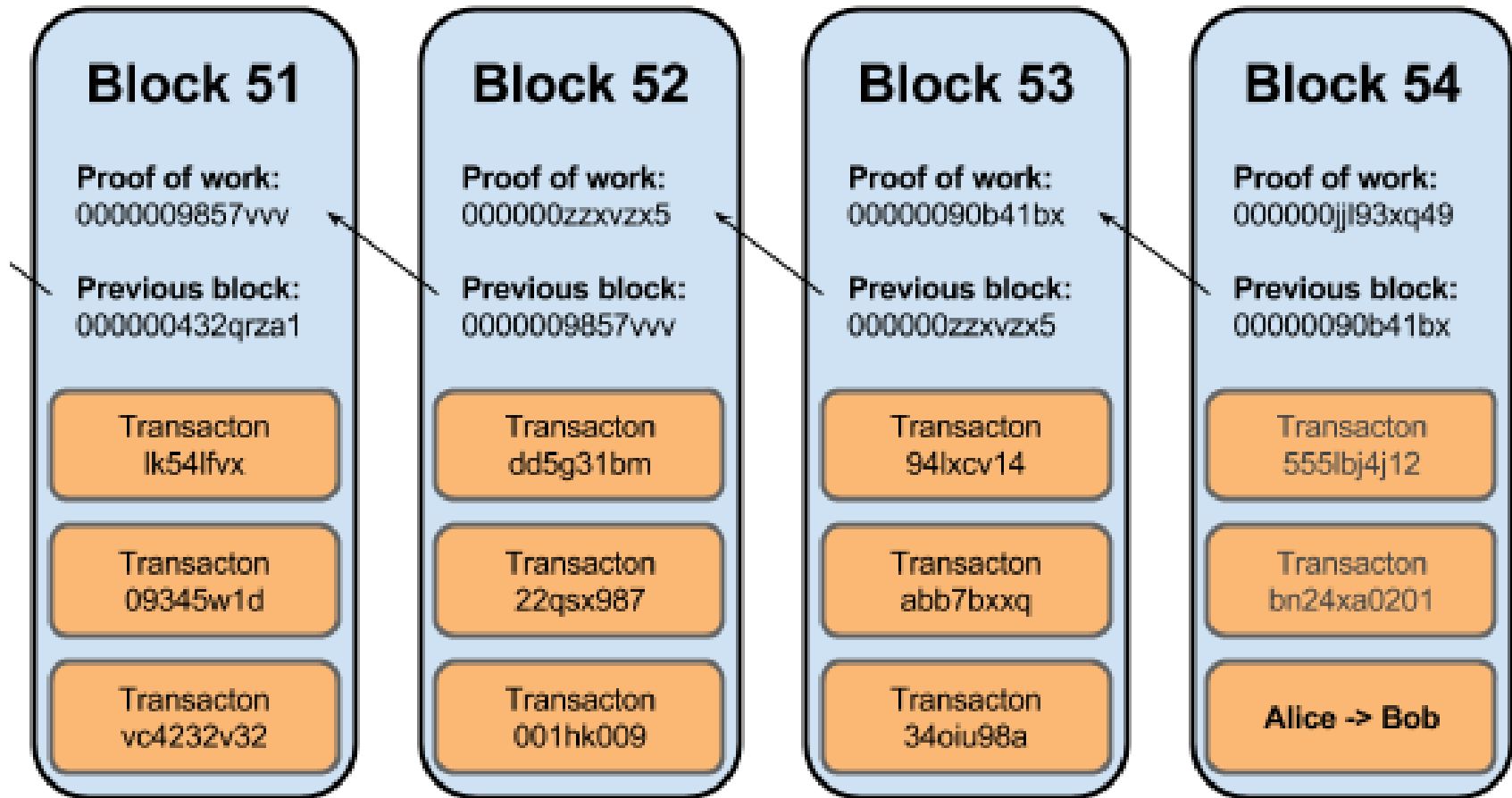
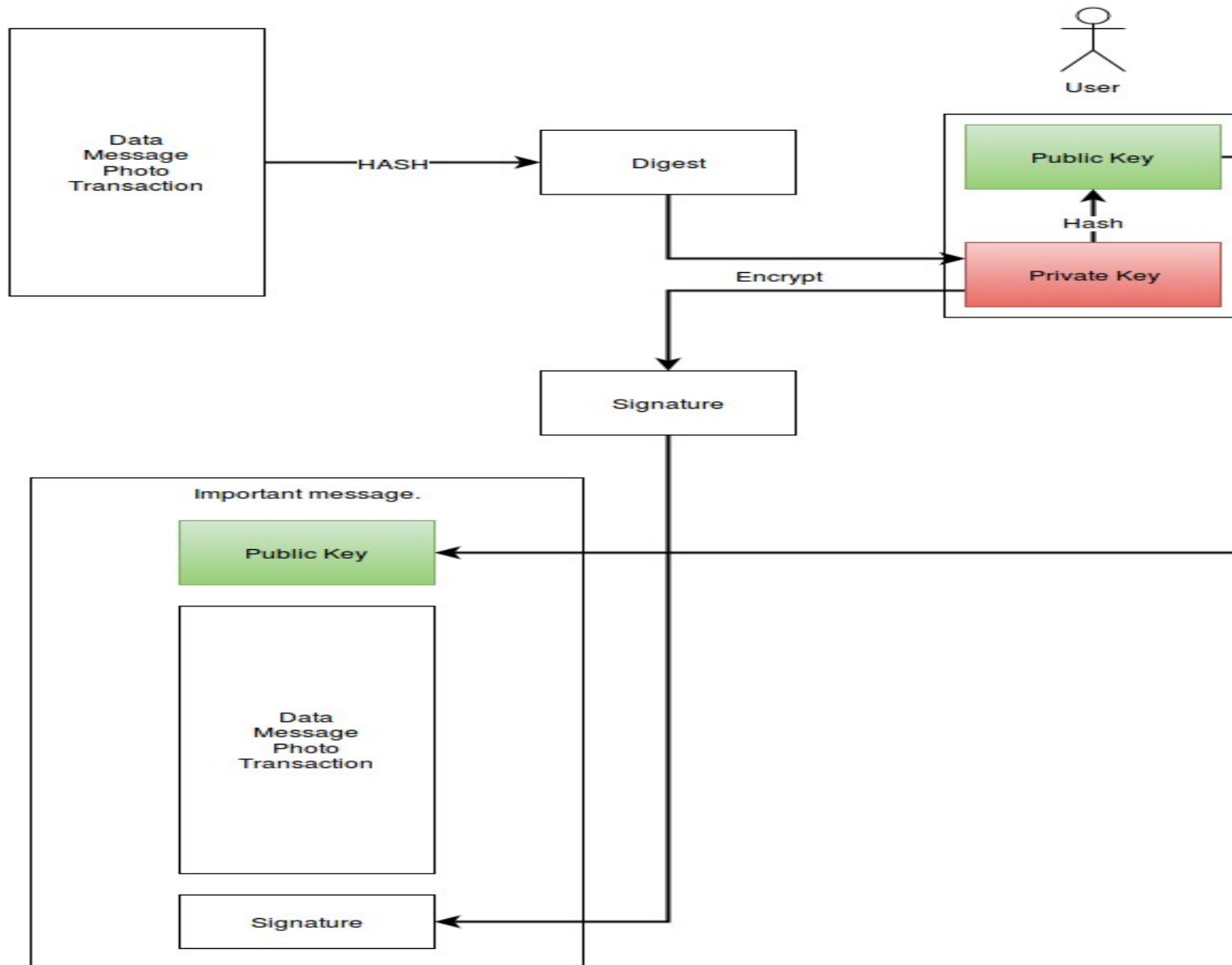


Fig. 2. The commander a traitor.

Blockchain=Solution



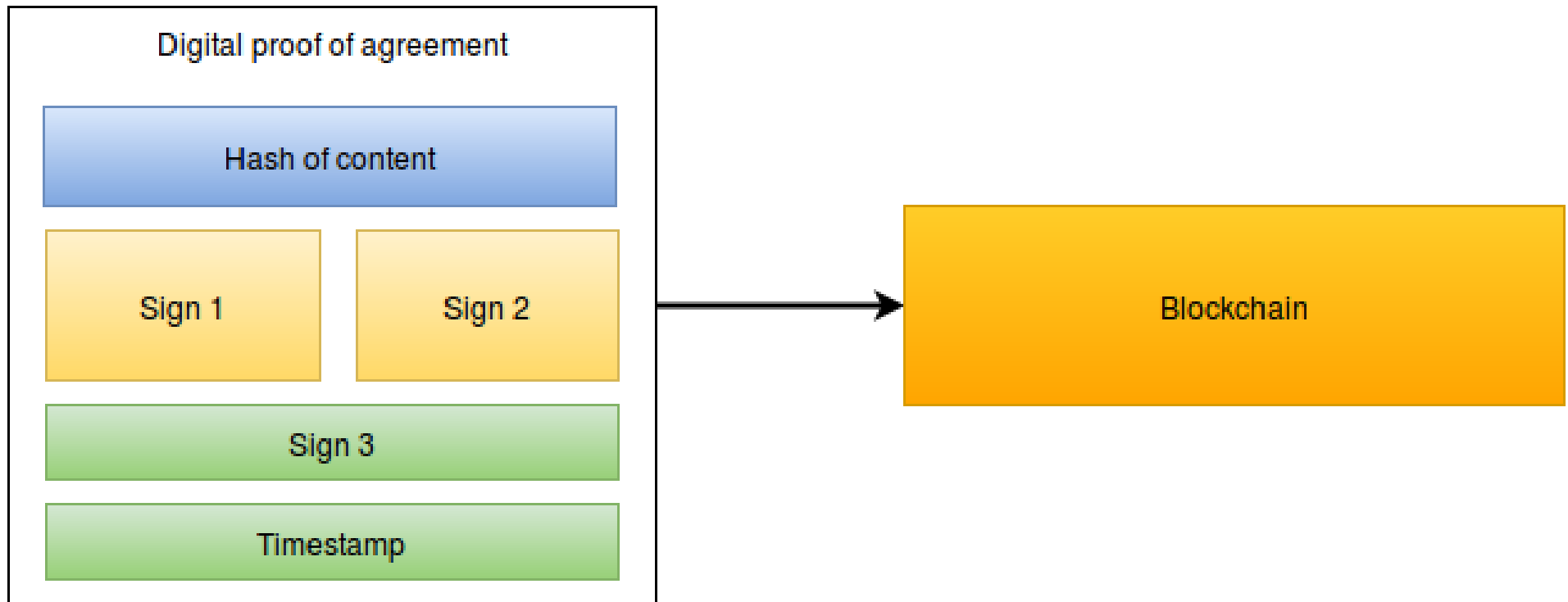
Transaction sign



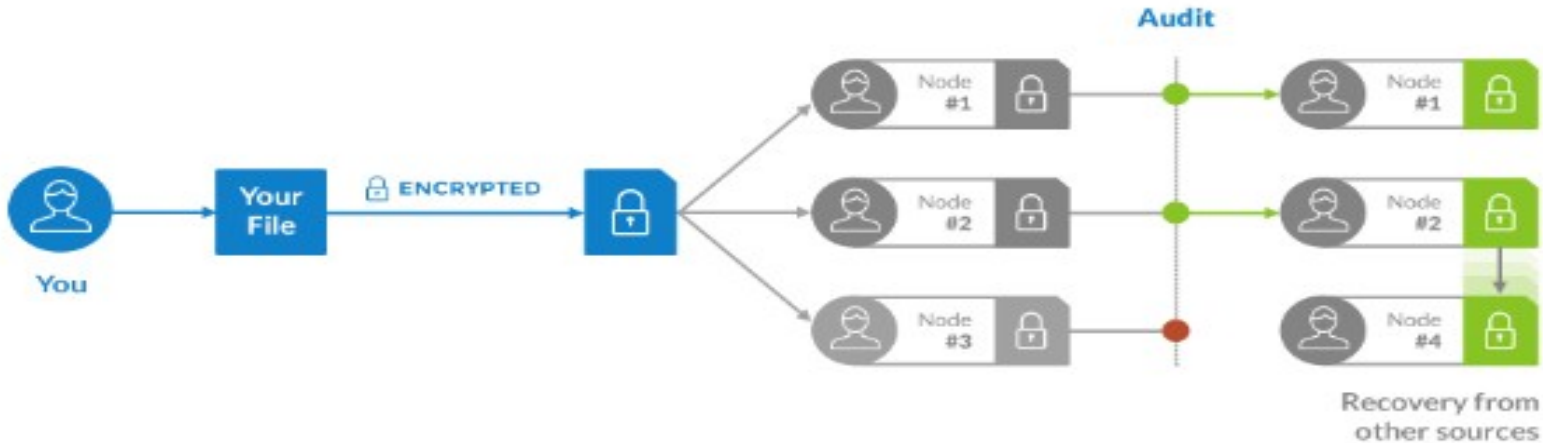
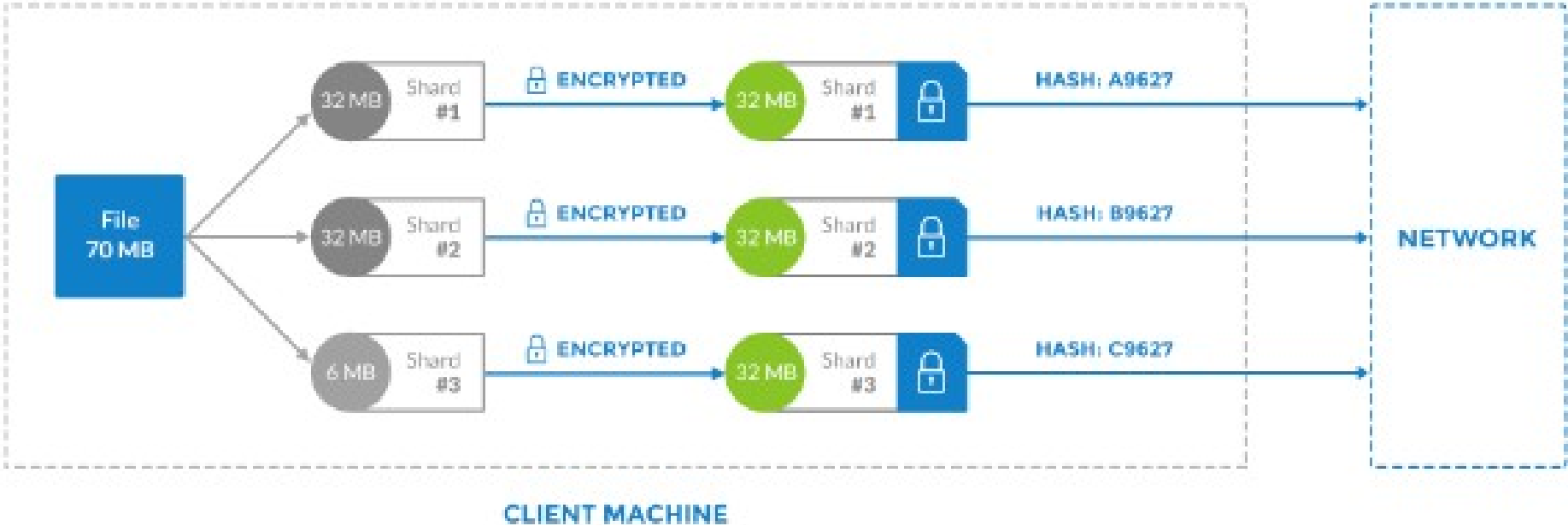
Possible applications

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

Digital document notarization



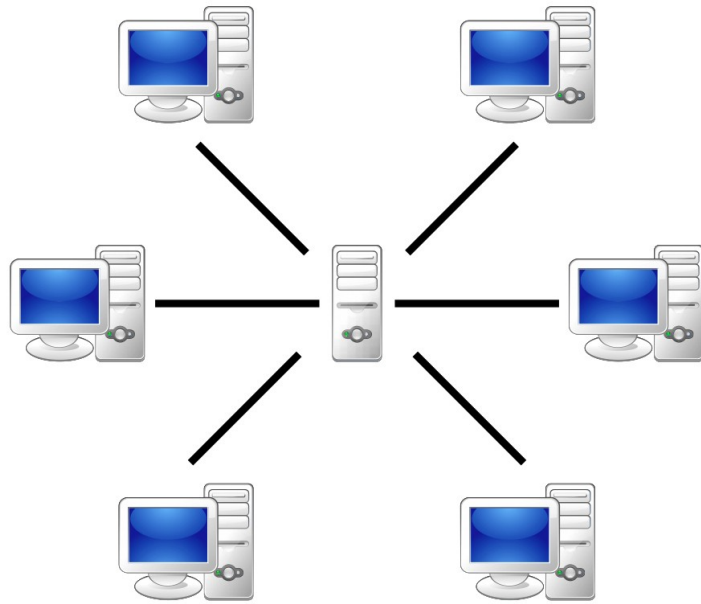
Distributed data cloud.



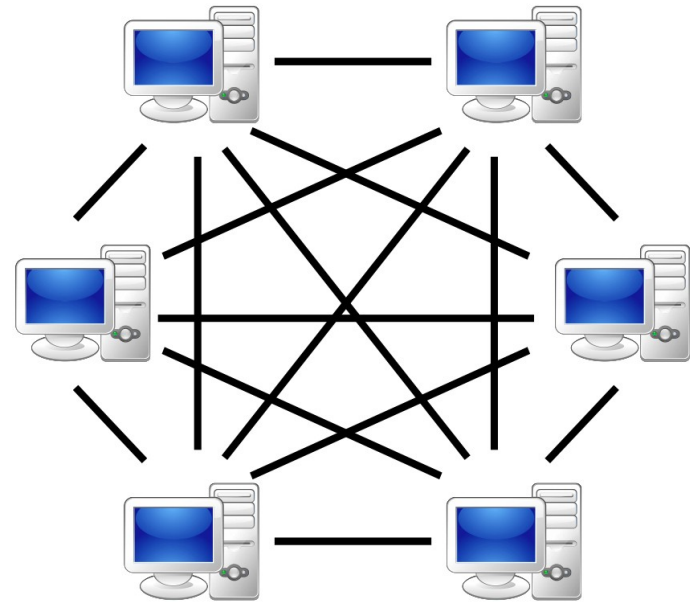
Infrastructure

- 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

Tim the creator of PGP (Pretty Good Privacy), a public-key encryption software package for the protection of electronic mail. Since PGP was published, occasionally as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of e-mail, sending countless industry secrets along the way. For three years I was the target of a relentless investigation by the US Customs Service, who convinced that there were trojans, when PGP spread outside the US. That investigation was closed without incident in January 1995.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were not in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the prewar-time attitudes toward cryptography today were learned in that period, and reverse the old attitude toward computers. Why would ordinary people need to have access to good cryptography?

Signature

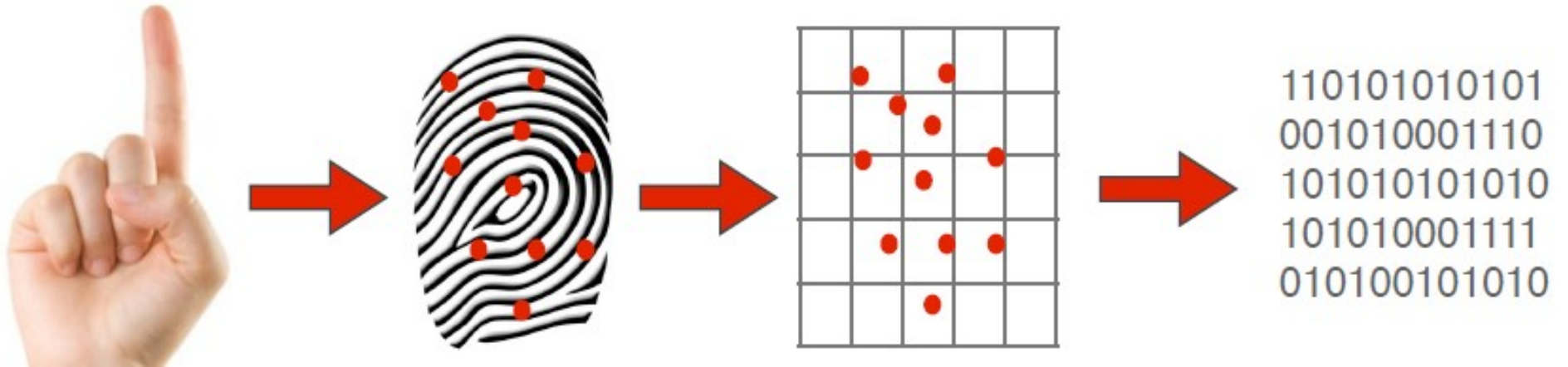
Hash

Message
Digest

Decrypt with
Public Key

Message
Digest

What about biometry?



Pros of Blockchain based technologies and applications

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

Q&A