DISCLAIMER

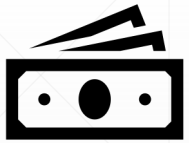
The content of this seminar is for informational and educational purposes only. You should not construe any such information, my opinions, and other material as legal, tax, investment, financial, or other advice.

A Brief History of Crypto

Money is continually evolving.

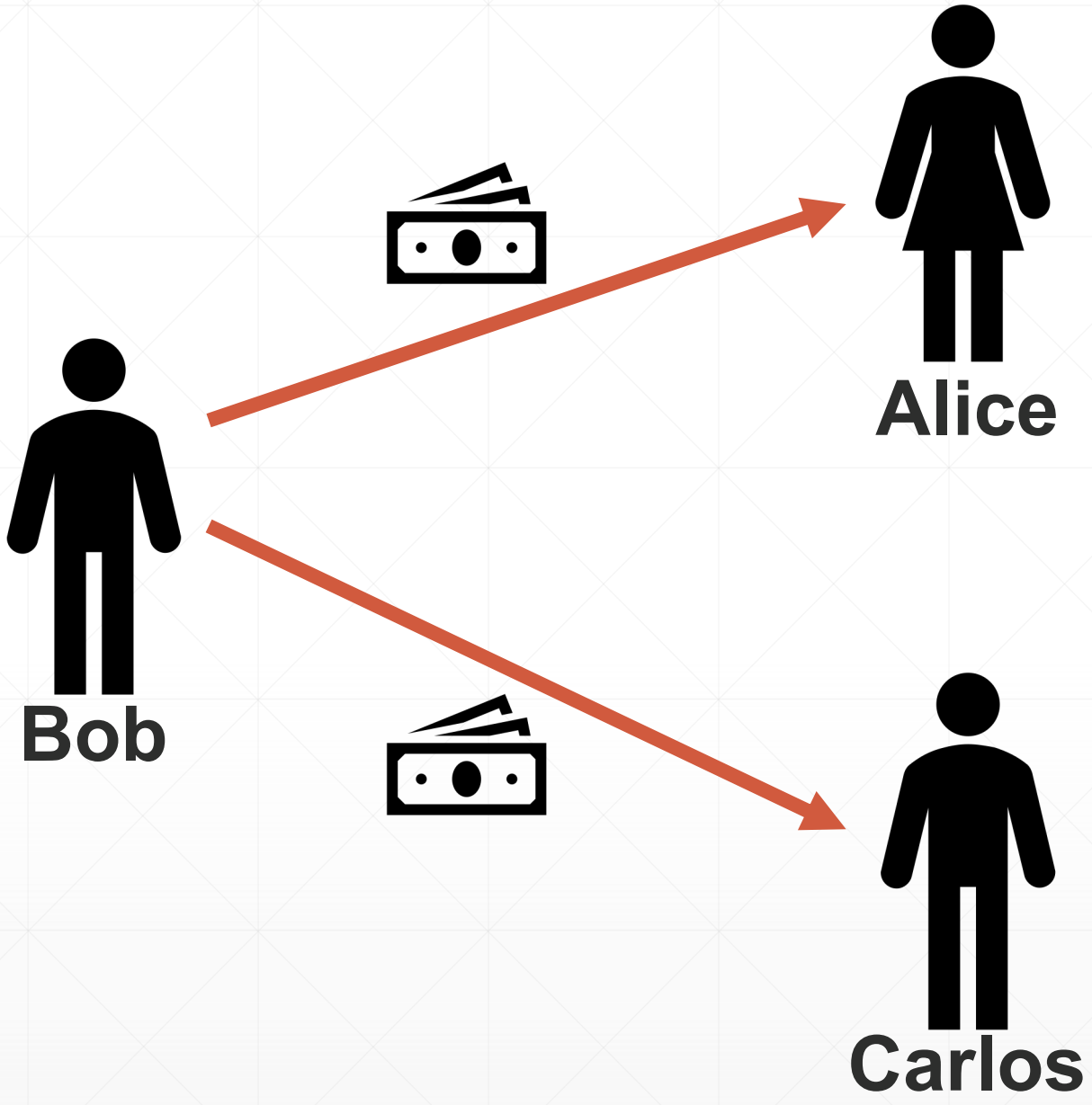
Barter → Metals → Paper → Plastic → Electronic → Digital






Digital money has a major challenge.

The double spend problem.


Alice
Bob
Carlos

2008.

The Great Recession.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

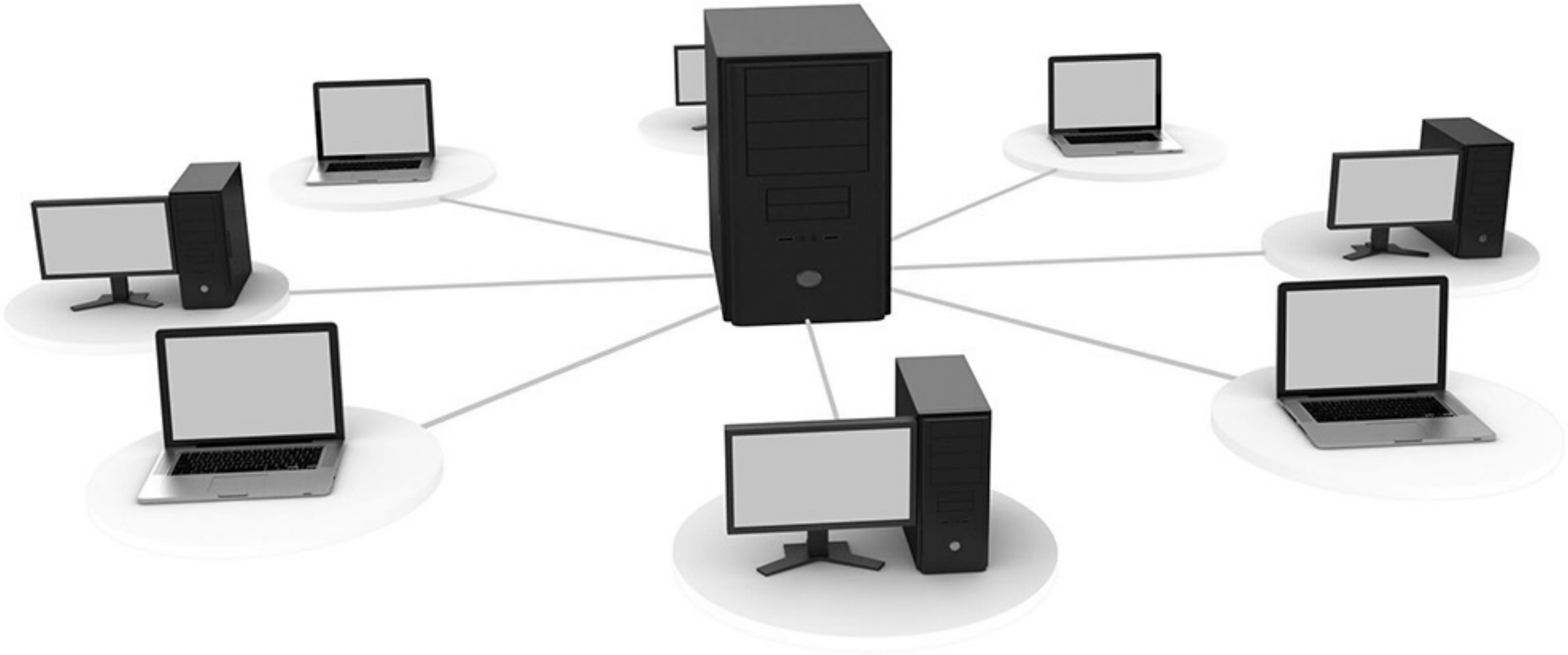
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

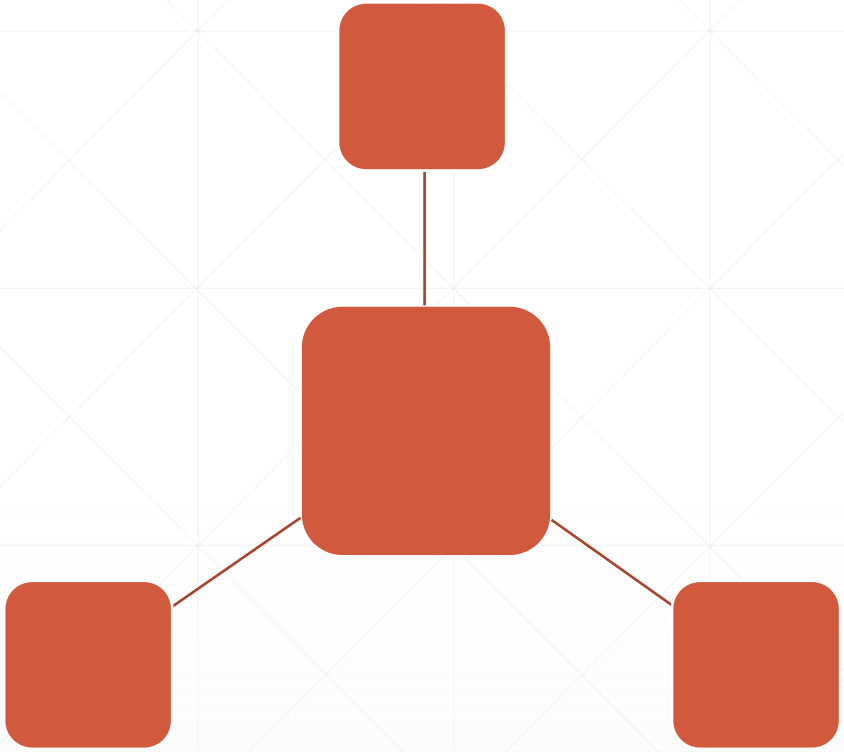
Bitcoin solves the double-spend problem.

And creates many more benefits!

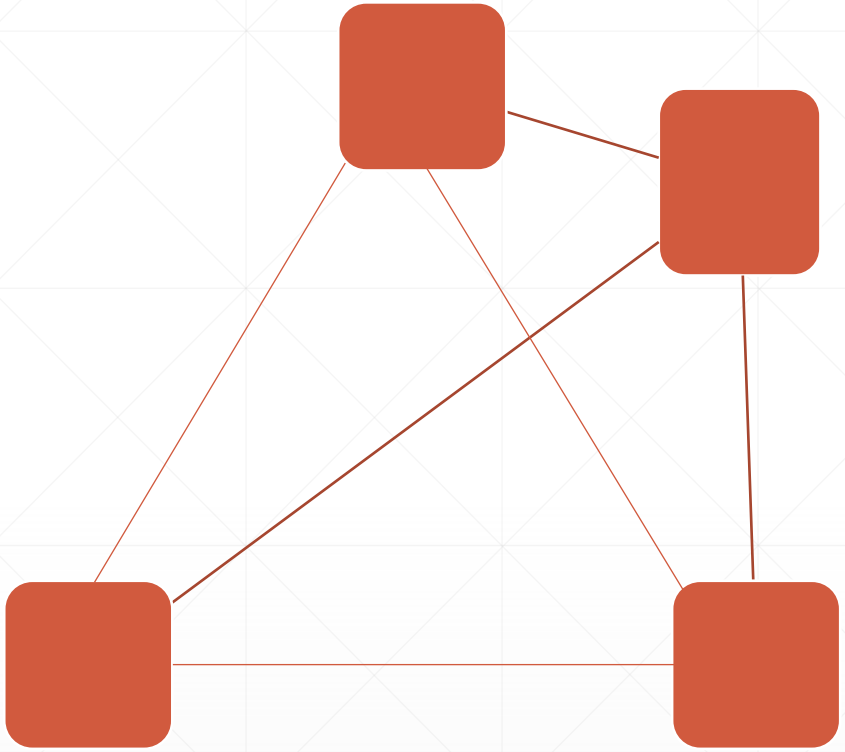
How can we ensure that all ledgers are kept current without any central trusted authority?

The Magic of Blockchain





Centralized

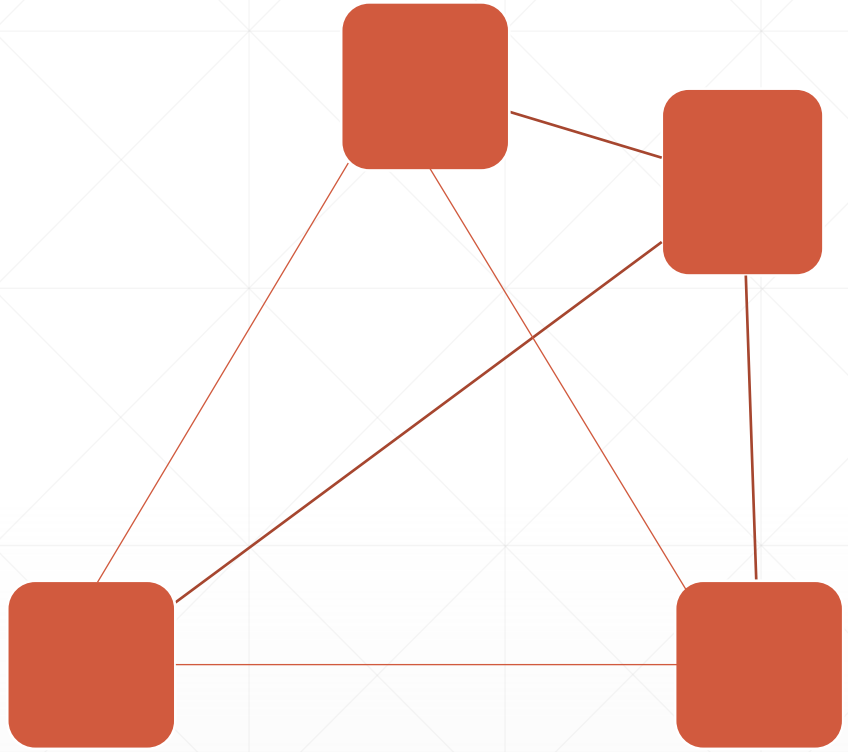


Distributed

What is a ledger?

A book in which business activities are recorded.

Distributed Ledger Technology (DLT)



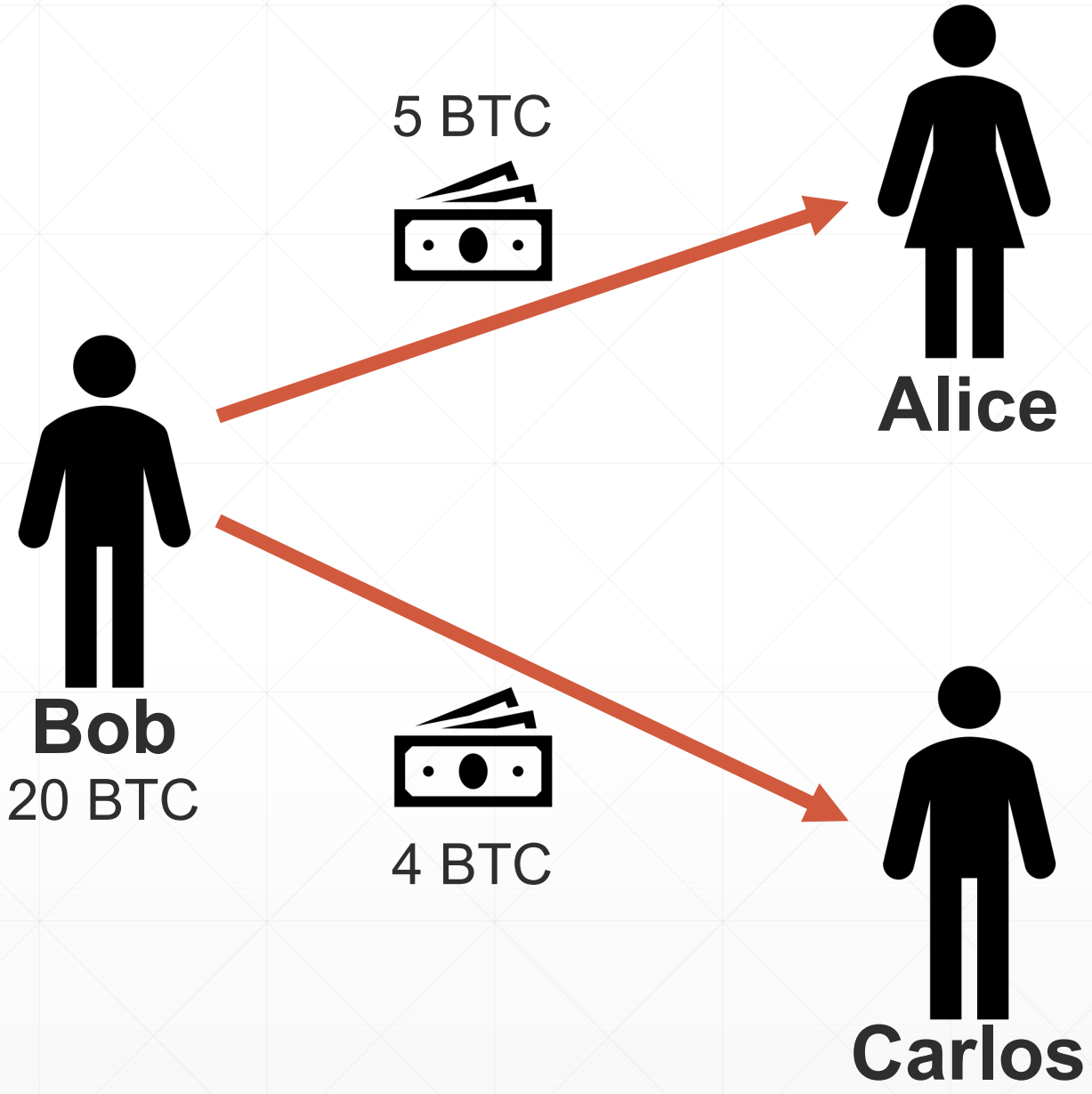
Distributed

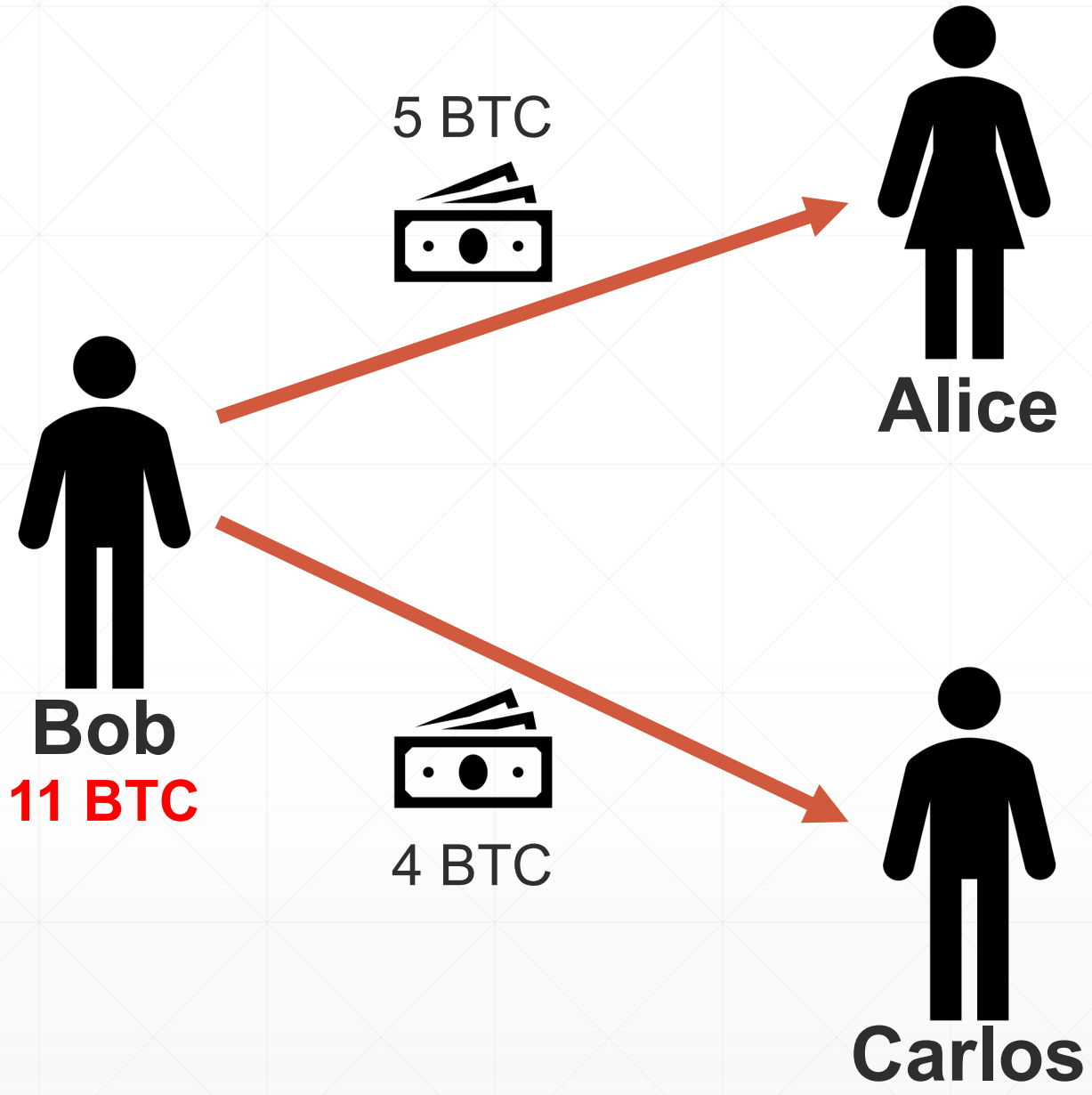
Blockchain is a type of DLT.

Each of them are a database.

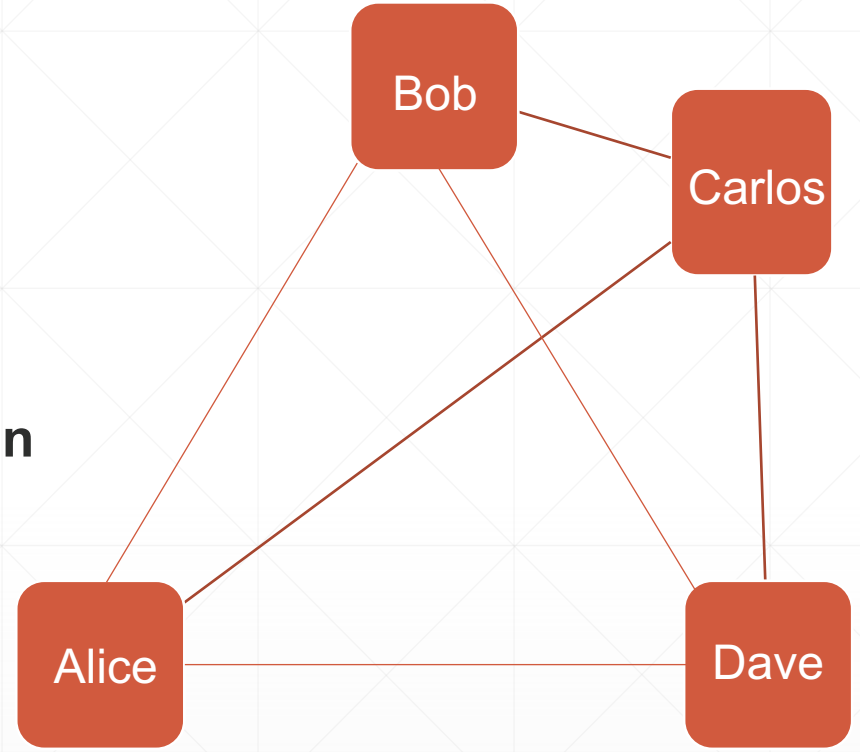
First Name	Last Name	Phone Number
Alice	Smith	987-123-2345
Bob	Jones	762-213-1122

Traditional Database	Blockchain Database
Centralized	Distributed
Modify records	Immutable (Non-modifiable)
Central management	No central management

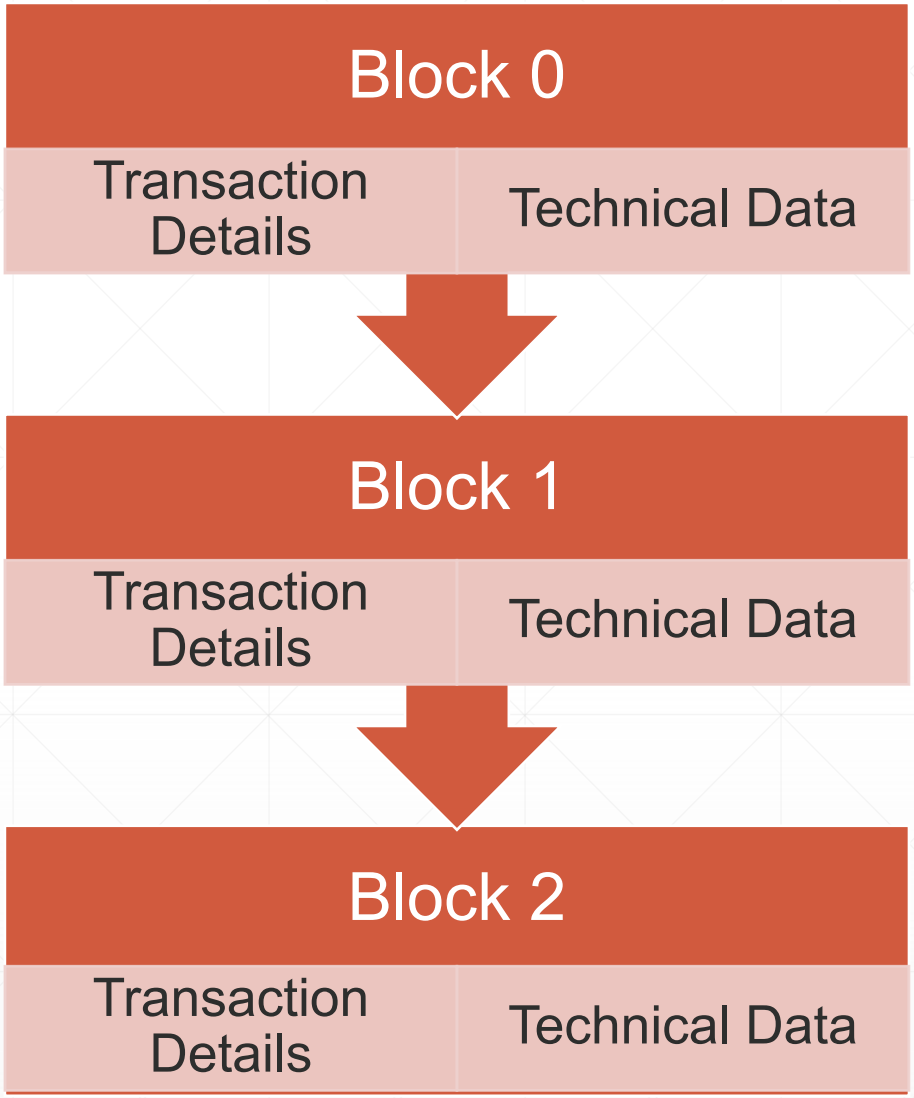

5 BTC
Alice
Bob
20 BTC
4 BTC
Carlos


5 BTC
Alice
Bob
11 BTC
4 BTC
Carlos

All users have a copy of the blockchain database
Bob broadcasts his payment request
Other users validate the transaction
A process then adds the transaction to the blockchain
All new transactions are then added to all users



Blockchain Network

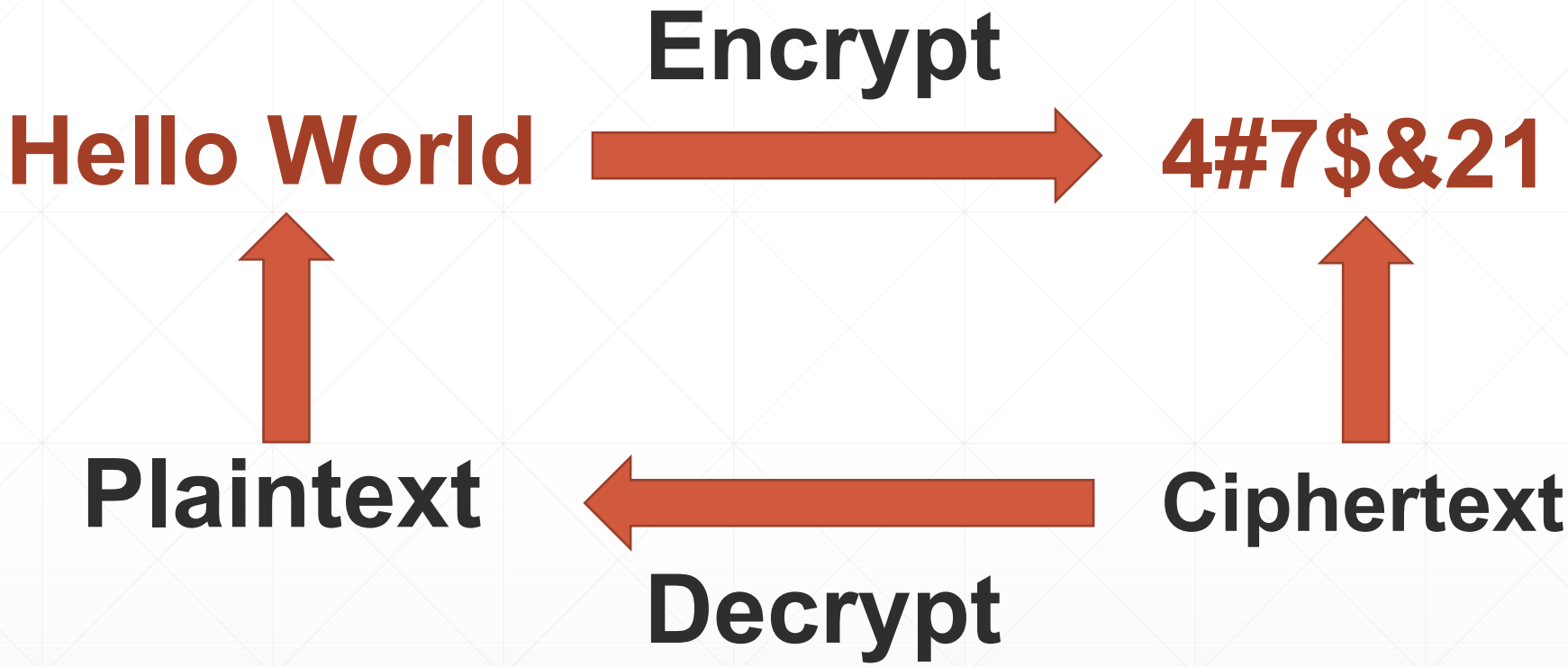


Each block depends on the previous one.

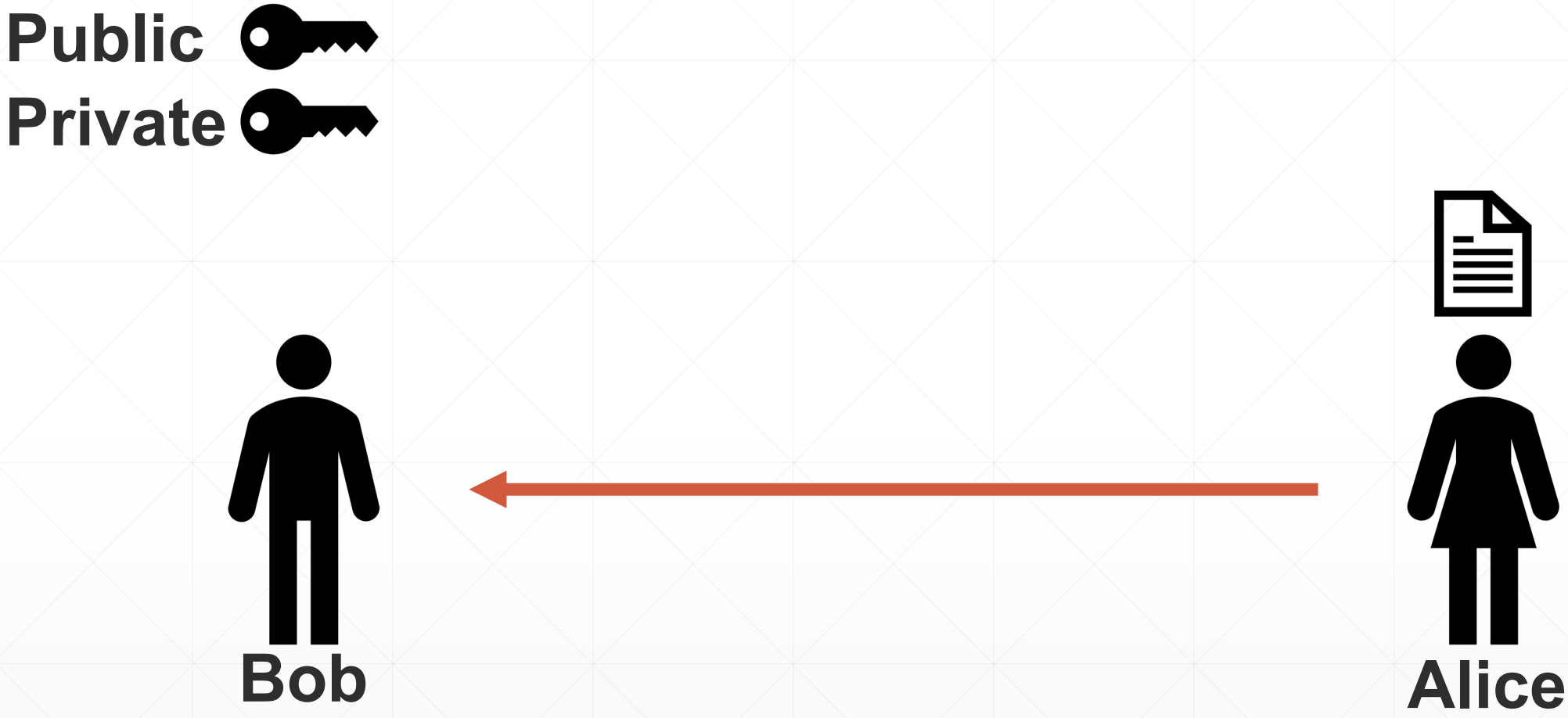
Blockchain is trustless and permissionless.

The Role of Cryptography

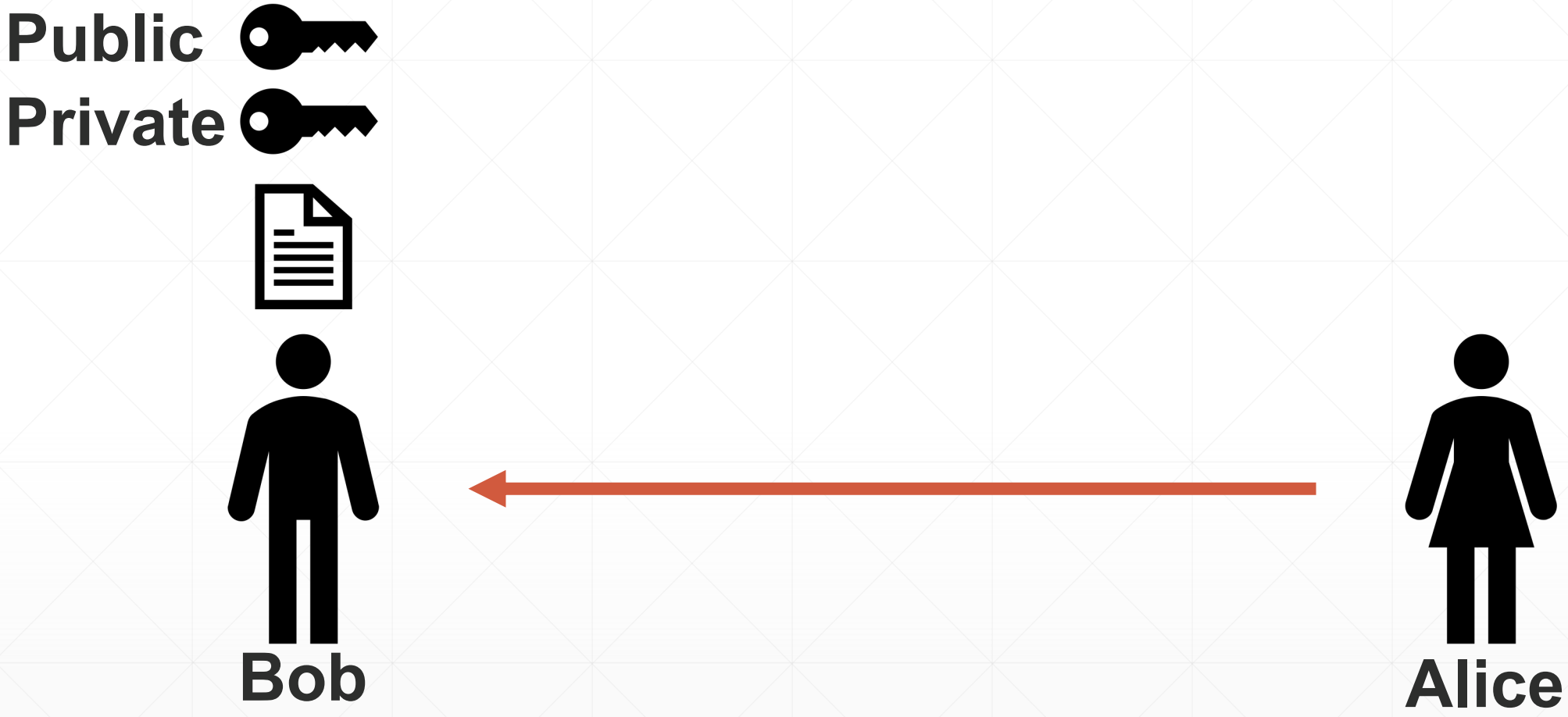
Cryptography is a Greek word that means secret writing.


Encrypt
Hello World
4#7$&21
Plaintext
Ciphertext
Decrypt

Alice wants to send encrypted document to Bob



Bob wants to prove the document is genuine



Private keys are stored in a wallet.

Blockchain Uses

Supplier
Ethical sourcing uncertain

Manufacturer
Environmental impacts unknown. Fragmented data systems and data loss

Regulator
Infrequent third party quality control

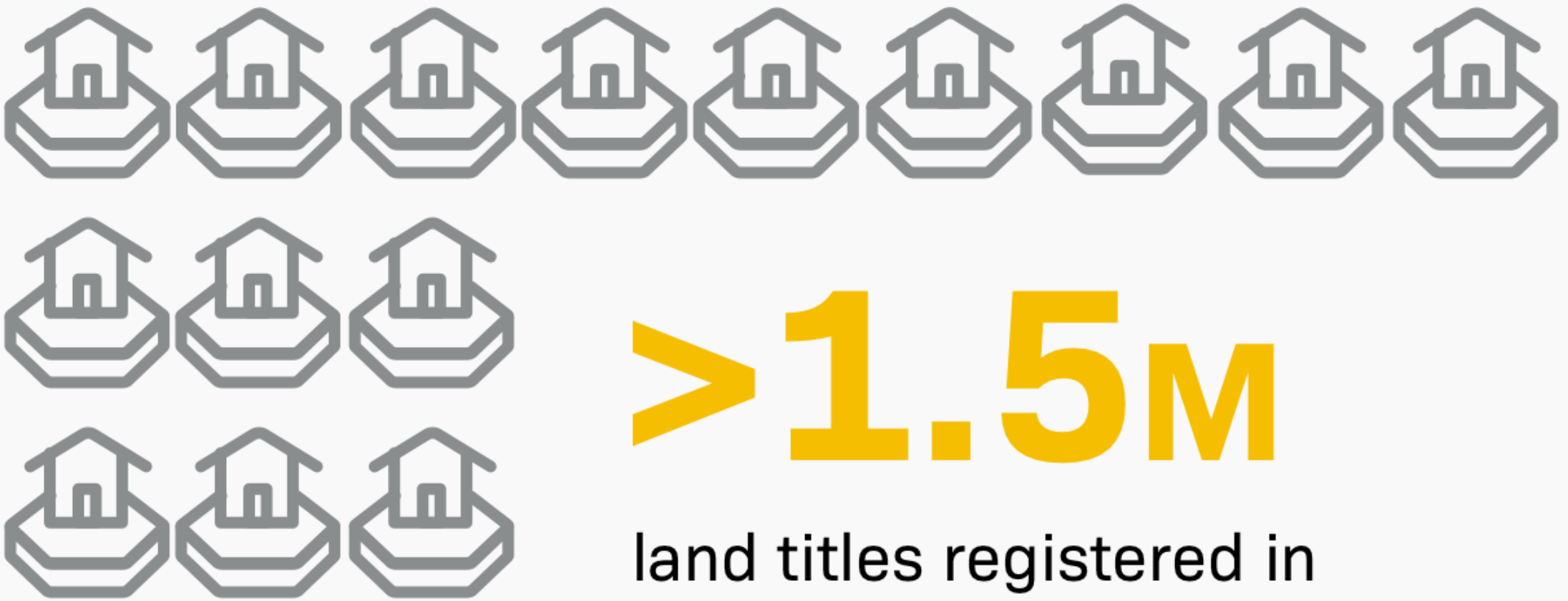
Logistics
Manual transport updates not in real-time

Wholesaler
Overstock and stockouts due to inaccurate supply and demand data

Retailer
Product provenance and authenticity uncertain

Consumer
Minimal supply chain insight


EESTI VABARIIK
Republic of Estonia
DIGITAALNE ISIKUTUNNISTUS
Digital Identity Card
BRONSTRING
MAREK
919409



>1.5M

land titles registered in blockchain

Storing & Managing Records

Professional licenses

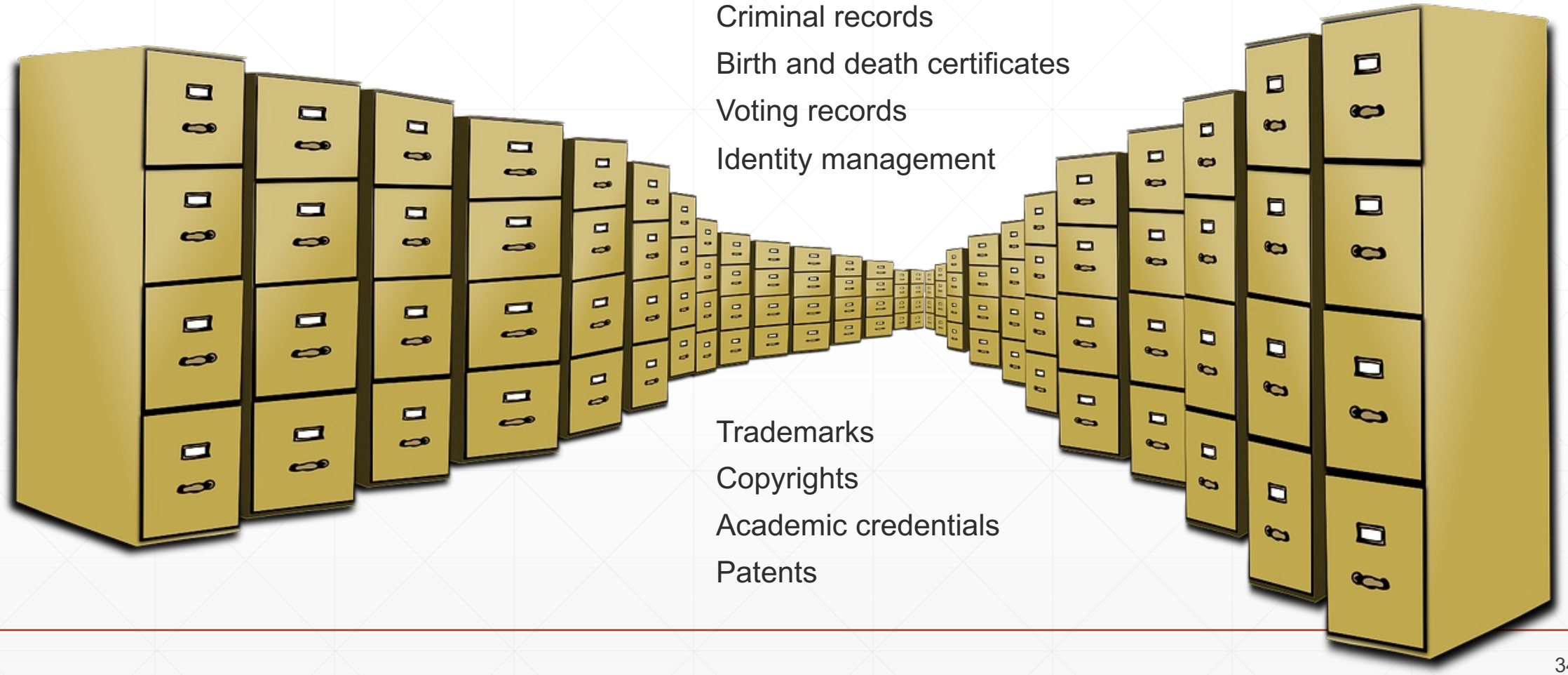
Tickets, fines, including payments and processing

Criminal records

Birth and death certificates

Voting records

Identity management



Trademarks

Copyrights

Academic credentials

Patents

Summary

- Bitcoin paper solved the double-spend problem
- Blockchain is a database that processes transactions
- Blockchain is distributed and immutable
- Transactions are cryptographically linked
- Private and public keys identify participants and transactions

Don’t lose your private key.

Questions?