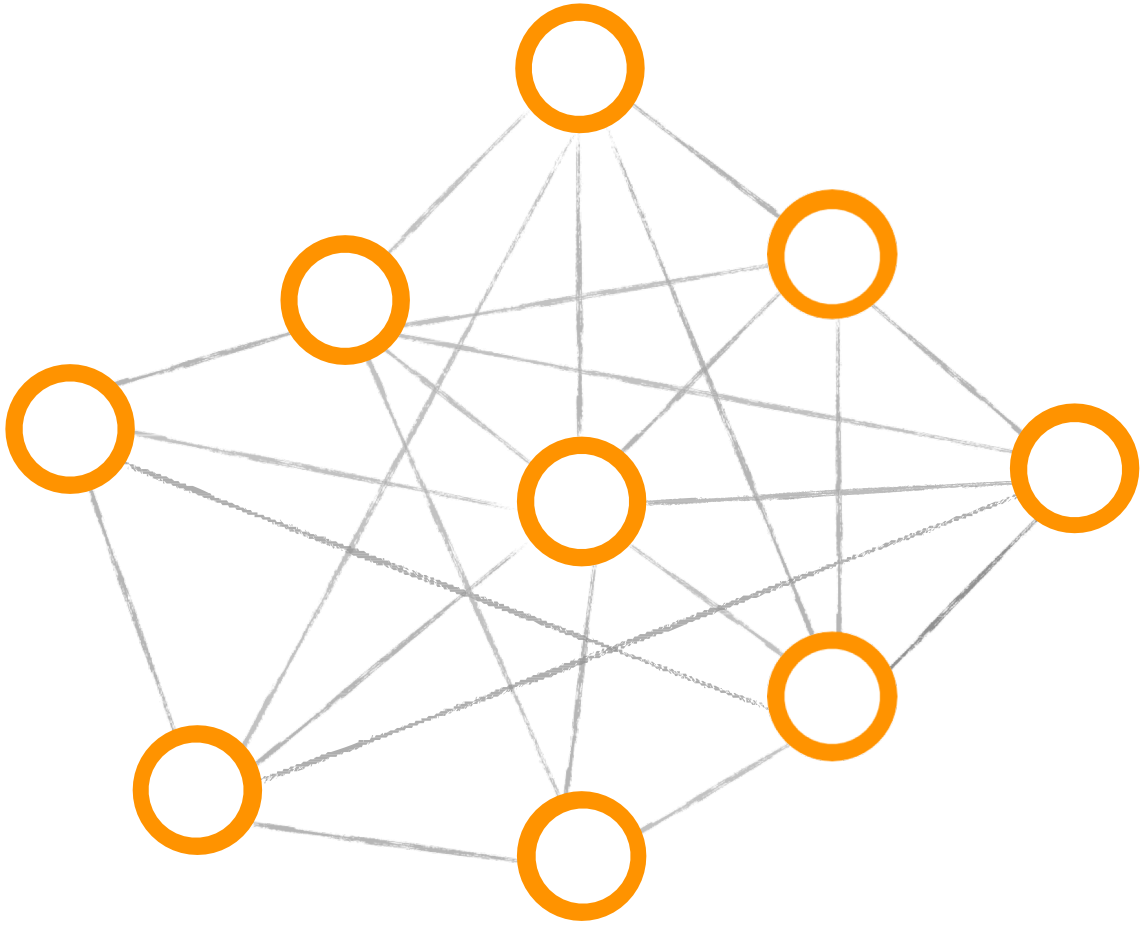
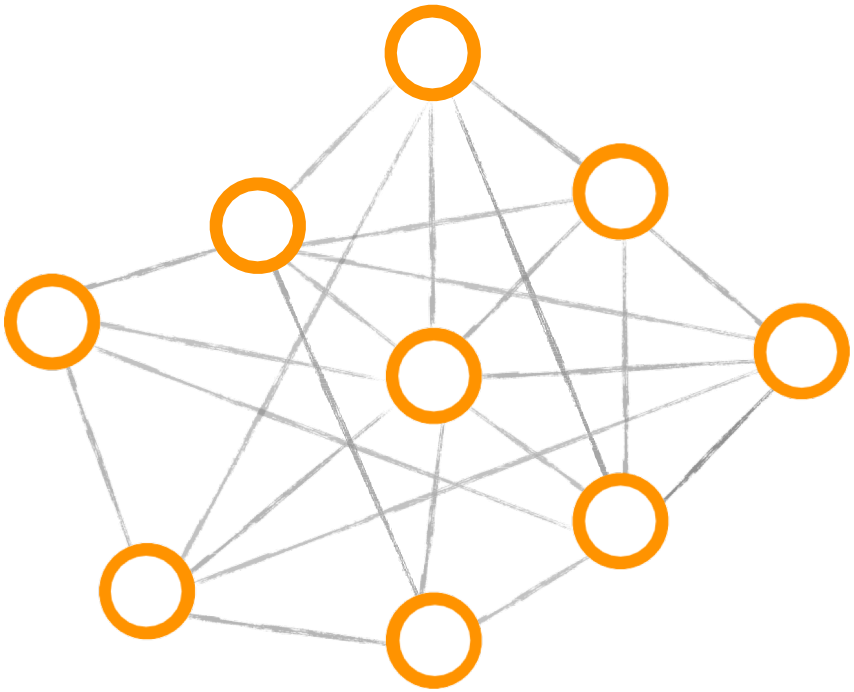
Demystifying the Blockchain

Myrna E. Amahan

What is Blockchain?

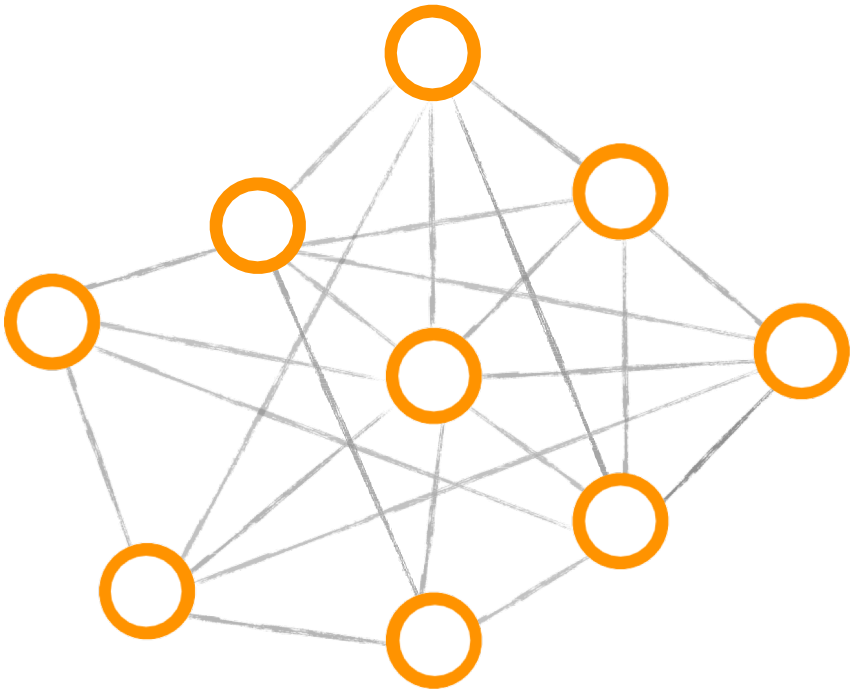
- Definitions
- How Blockchain Works
- Security
- Use Cases





What is Blockchain?

The technology that powers Bitcoin. While this was the original purpose, blockchain is capable of so much more.



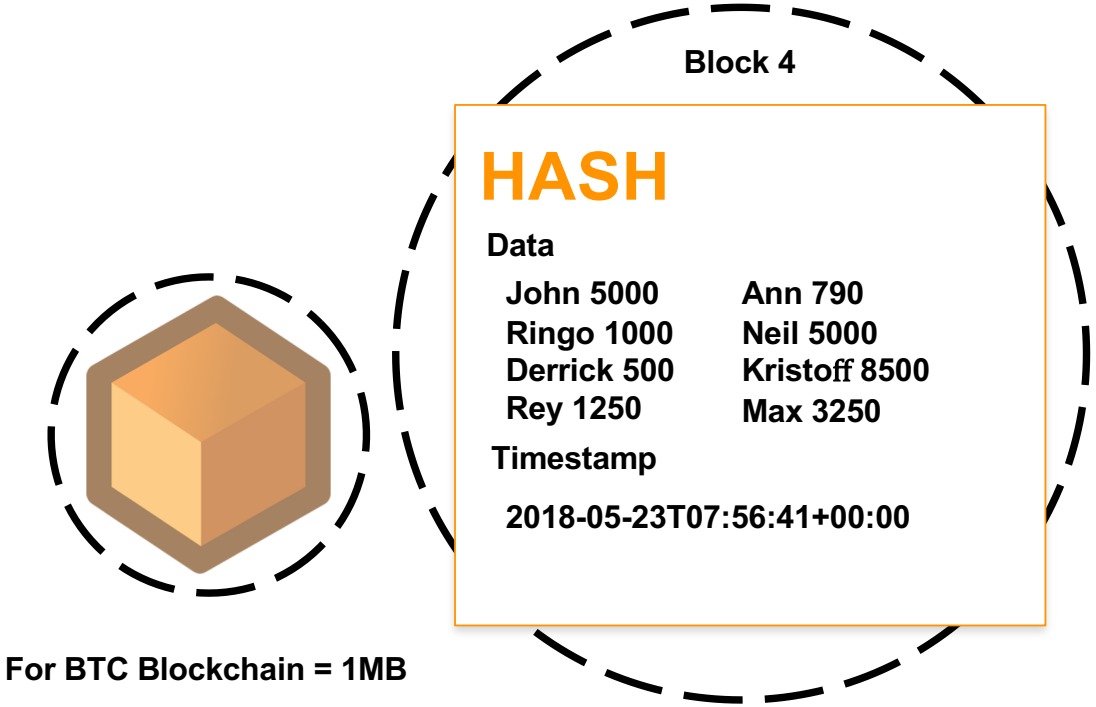
What is Blockchain?

is a *persistent, transparent, append-only* ledger.

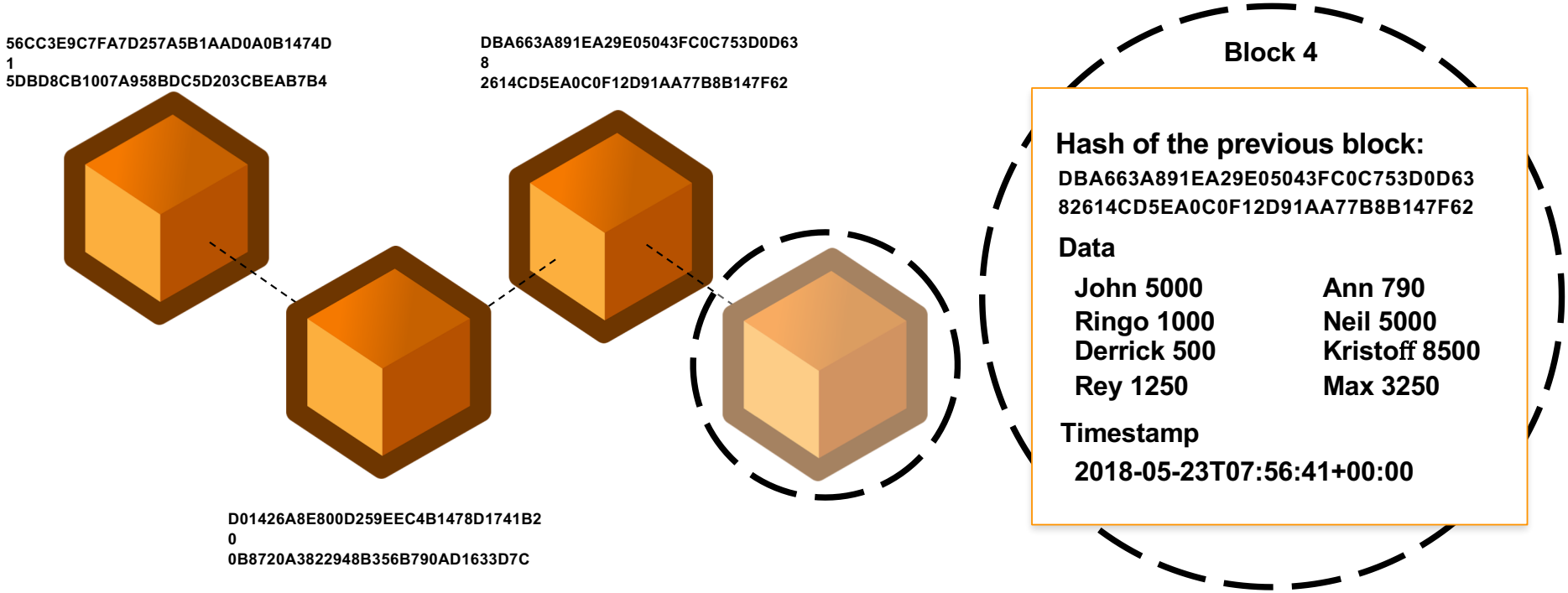
Simply, it is a system that allows you to record data in it (which can be anything of value) but ***not*** change previous data within it.

Data are stored in “blocks” of information and existing data is based on previous data, thus forming a “chain” of information hence “blockchain”.

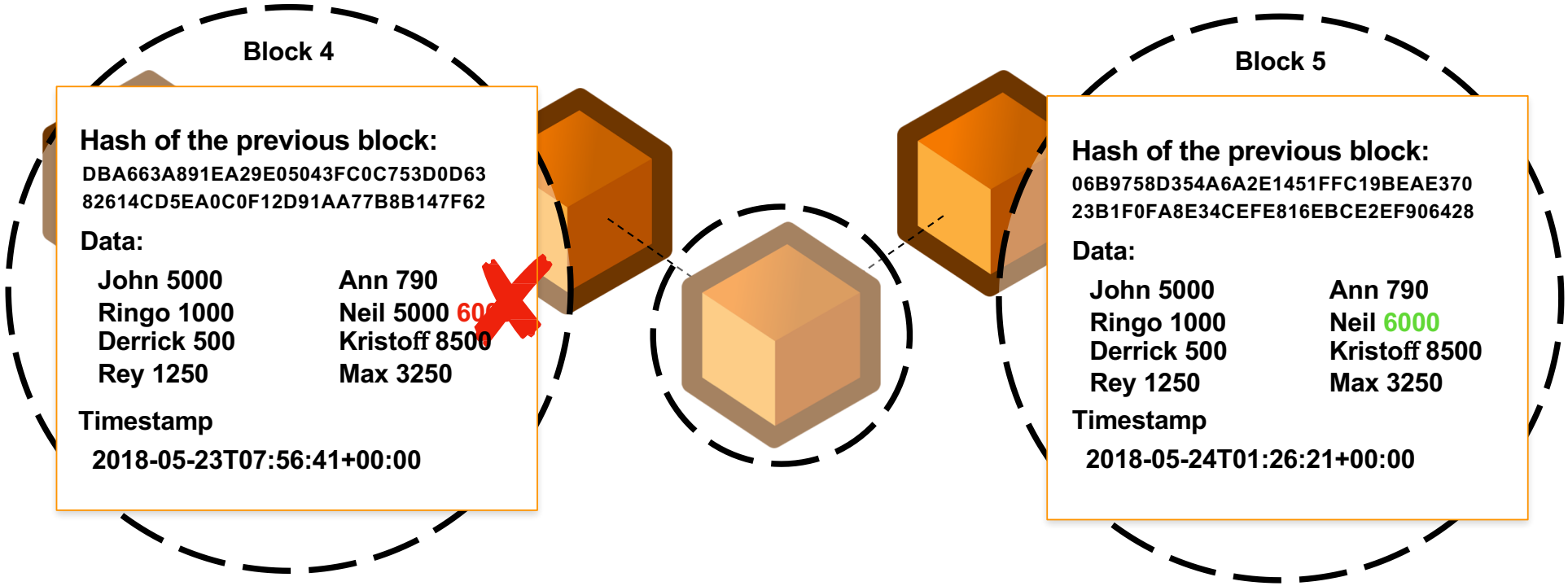
WIRED. "Blockchain Expert Explains One Concept in 5 Levels of Difficulty | WIRED." YouTube. November 28, 2017. Accessed May 03, 2019. https://www.youtube.com/watch?v=hYip_Vuv8J0



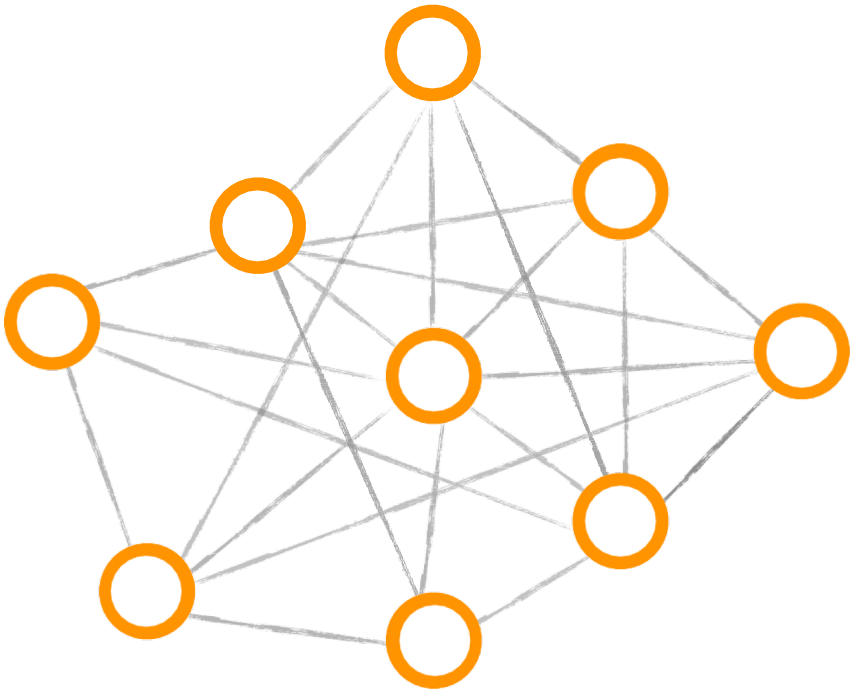
Data are stored in batches, called blocks



Chain of blocks = blockchain



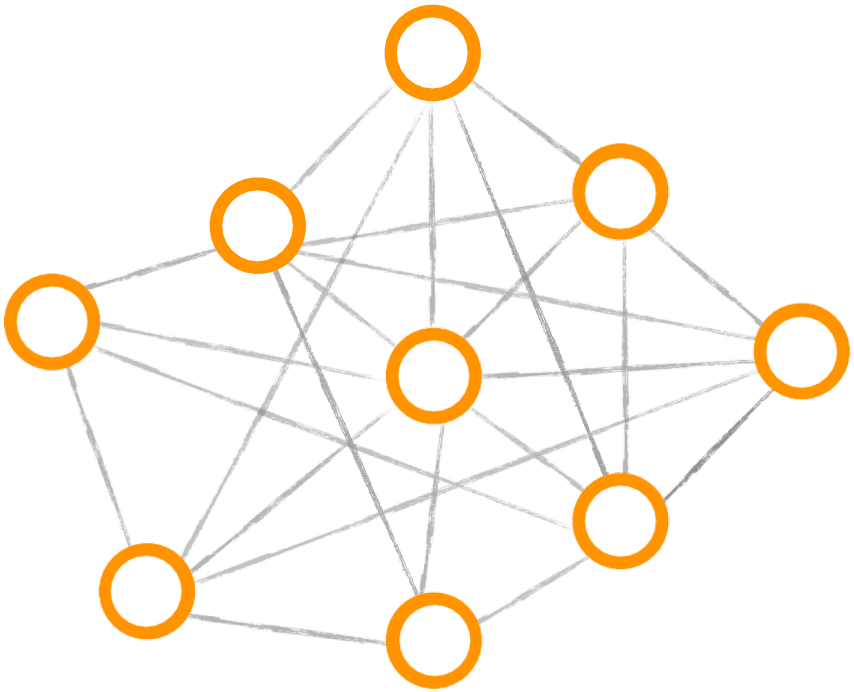
No update/delete on blockchains, append only storage



What is it used for?

Since any data can be stored in the Blockchain, it can be used for many purposes.

Examples of data that can be stored include financial transactions, medical records, transparent land titles, personal identity, and more.



Why is Blockchain important?

Almost all systems/institutions rely on *trust*, but Blockchain is revolutionary because the entire system is *trustless*.

This means that no middle-men are required to verify the authenticity of data, therefore cutting bureaucracy and making everything more efficient.

Examples of Trusted Middlemen

Finance

- Banks
- Exchanges
- Insurance
- Venture Cap
- Remittance & FX
- PayPal

Governance

- BSP
- Justice System
- Land Registry
- NSO
- BIR
- COMELEC

Online

- Google
- Yahoo
- Facebook
- Amazon
- eBay
- LinkedIn

Brokerages

- Real Estate
- Investment
- Trading
- Mortgage
- Logistics & Customs

Charity & Foundations

- PCSO
- Non-profits
- Donations
- Red Cross
- Crowdfunding

Middlemen or Facilitators

Features of Centralized Systems

Party A

Participants of an ecosystem or transaction

Middleman

Facilitator, record-keeper, and usually an authority

Party B

Participants of an ecosystem or transaction

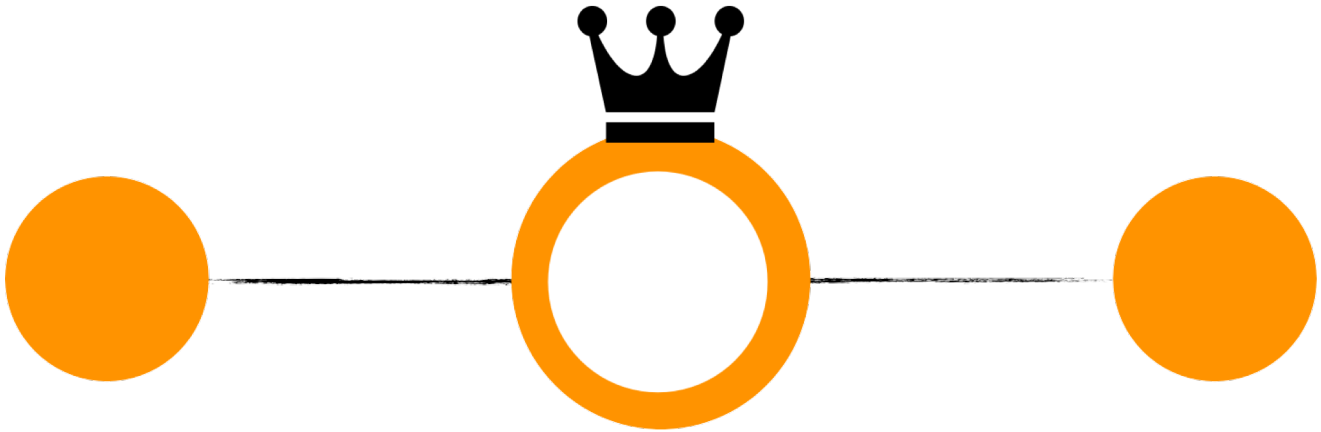
Gatekeeping

Features of Centralized Systems

Single Source of Truth

Can be corruptible, Censorable and Deletable

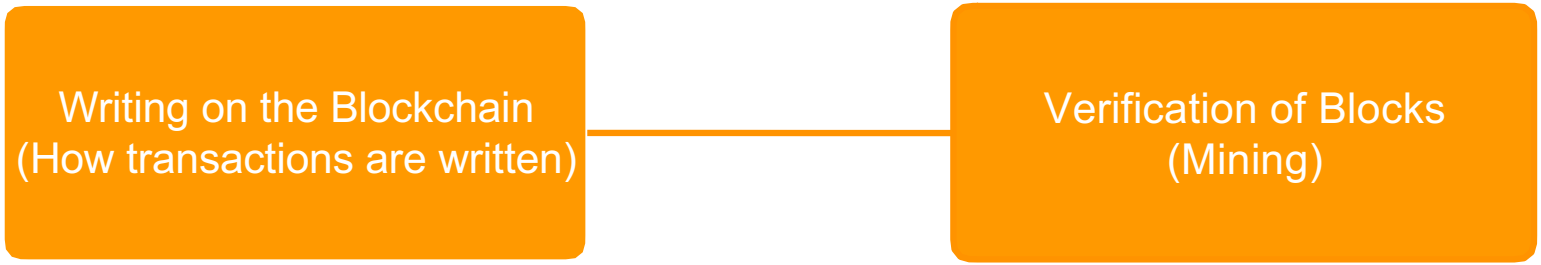
Features of Centralized Systems

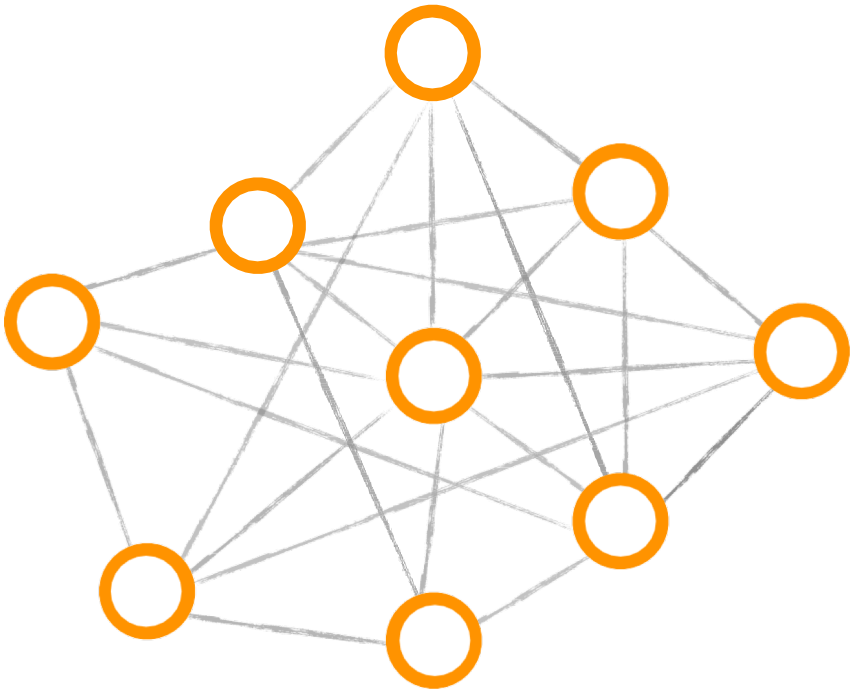


Control

Too much responsibility (and power) on one entity;

How does Blockchain work?





How does Blockchain work?

It works like a ledger. In a real ledger, transactions are recorded per page, and the pages will be verified as correct by a trusted third-party (e.g. a third-party auditor).

In Blockchain, it works the same way. Pages are the blocks of transactions and the seal needed to certify a book of transactions is correct is called the hash function. And instead of a separate third-party, transactions in Blockchain are verified by miners.

Mamoria, Mohit. "WTF Is The Blockchain?" Hacker Noon. June 30, 2017. Accessed May 03, 2019. https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348.

What is a hash

A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided.

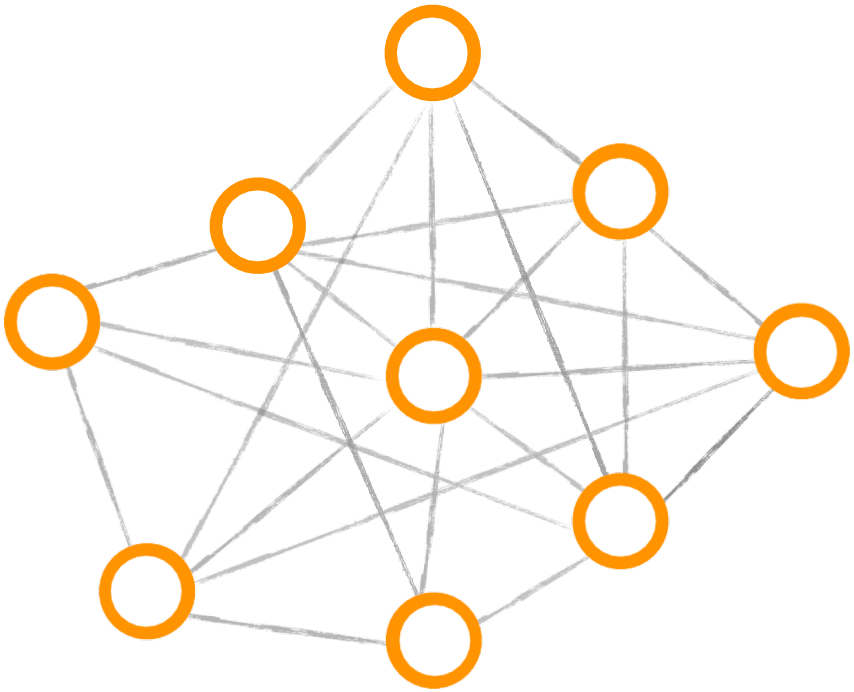
If at least one character is changed from the input, the output will change.

SHA-256 HASH

Text Input	SHA-256 Output
The quick brown fox jumps over the lazy dog	d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e92
The quick brown fox jumps over the lazy dog.	ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.	2d8c2f6d978ca21712b5f6de36c9d31fa8e96a4fa5d8ff8b0188dfb9e7c171bab

Comparison

Ledger	Blockchain
Page of transactions	Block of transactions
Seal of assurance (e.g. signature)	Hash functions
Third-party verifier	Miners

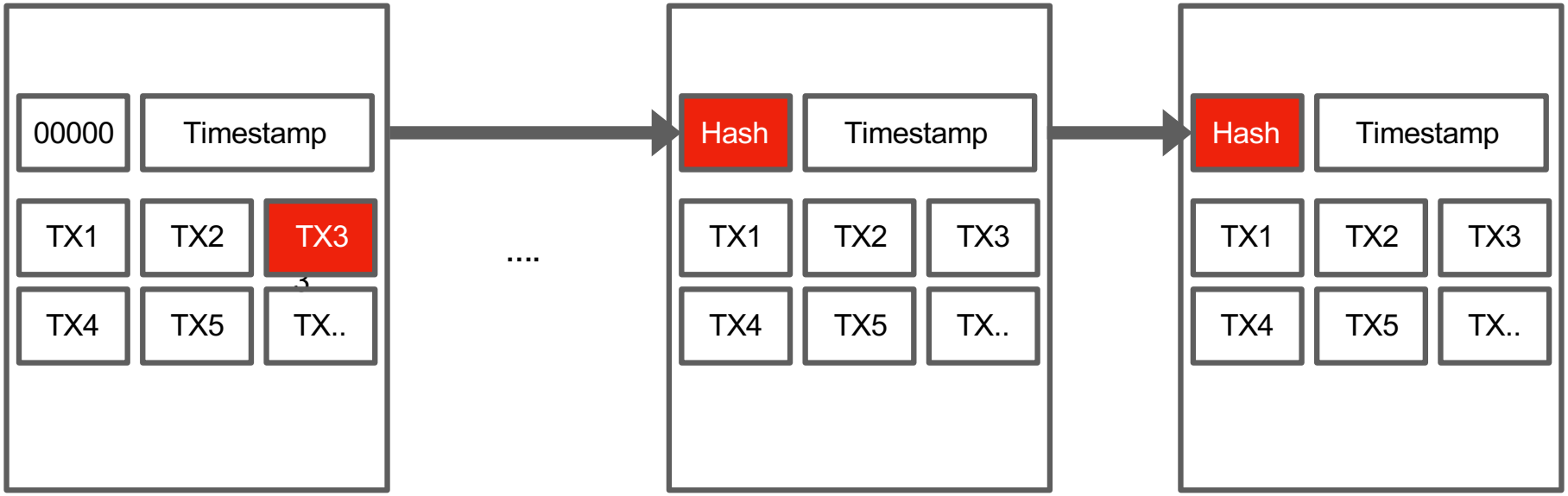


How are transactions recorded?

To record transactions in the Blockchain, transactions are “announced” in the network and go into blocks to be verified.

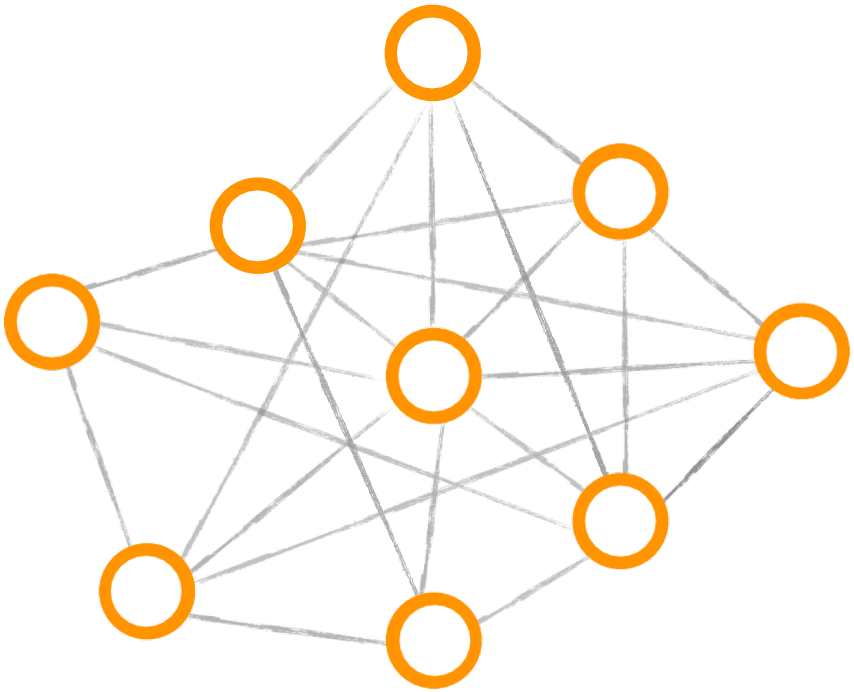
Aside from the transactions, to seal a block, it needs to include the hash of the previous transaction in order to be valid block.

Blockchain


00000
Timestamp
TX1
TX2
TX3
TX4
TX5
TX..
....
Hash
Timestamp
TX1
TX2
TX3
TX4
TX5
TX..
Hash
Timestamp
TX1
TX2
TX3
TX4
TX5
TX..
Block 0
Previous Block
Latest Block

What is *Mining?*

Mining is the process of verifying new transactions and tokens into the network to ensure they are valid single-spend transactions only

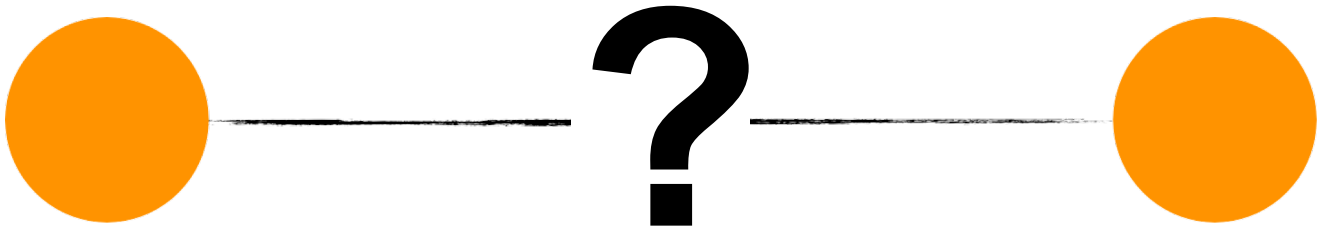


How then are blocks validated?

Once transactions are placed in a block, they need to be validated.

Miners step in to verify transactions. By design, the network requires miners to solve a mathematical problem in order for the block of transactions to be added to the chain. The first to solve this problem gets a reward and can "append" the block to the chain.

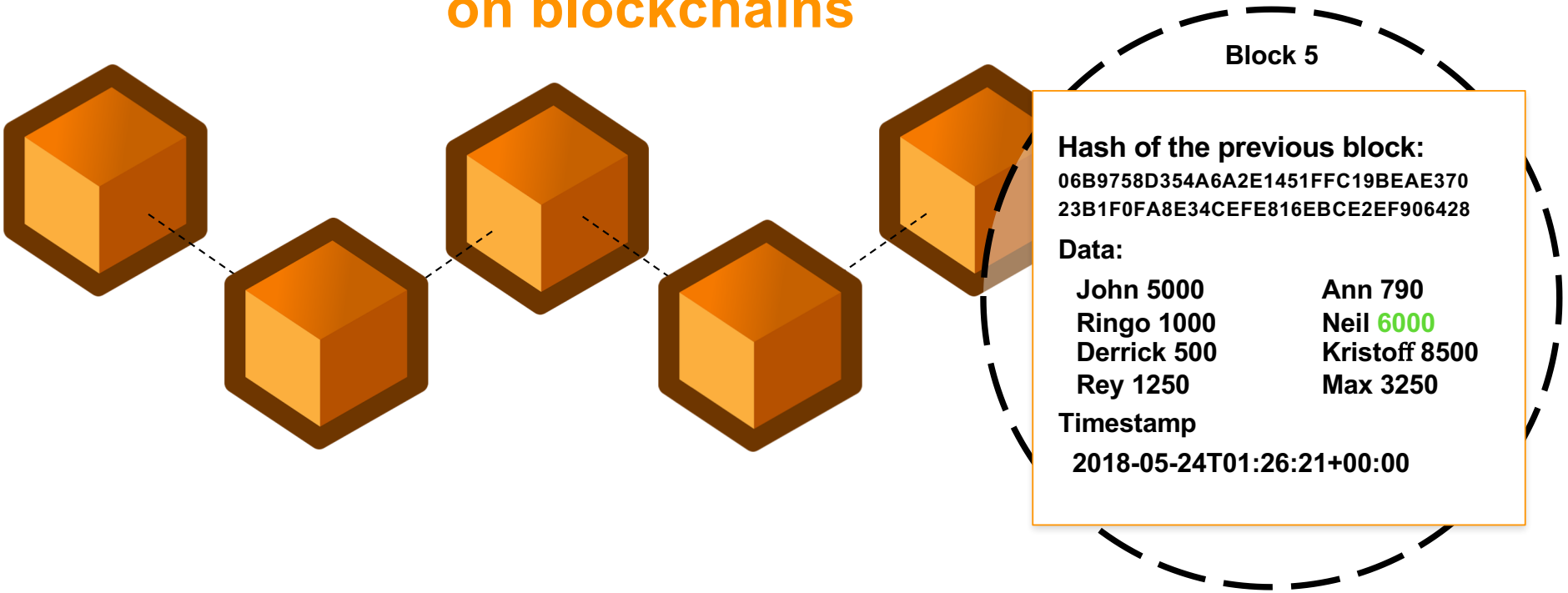
The process of solving is called *mining and the* solution to this problem is called the *proof of work*.



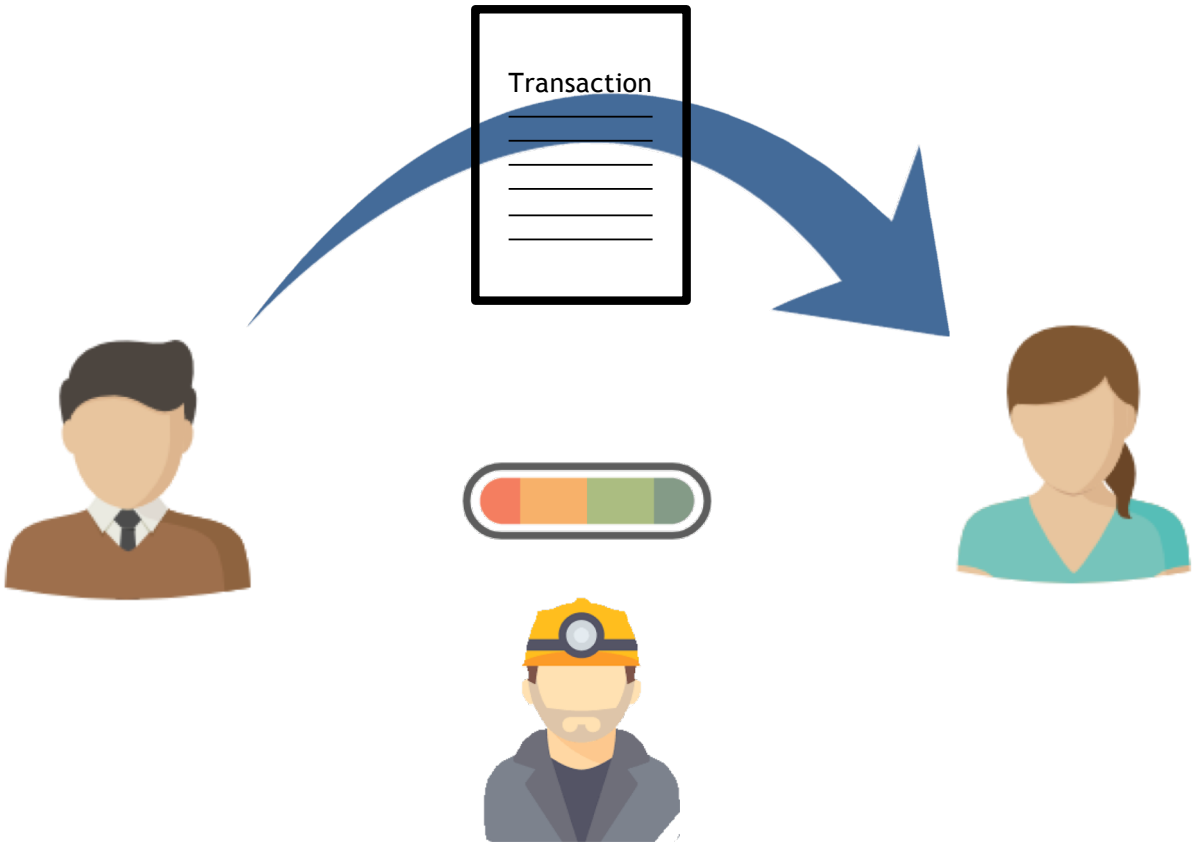
Who monitors the transactions on blockchains?

Participants (e.g. Miners)

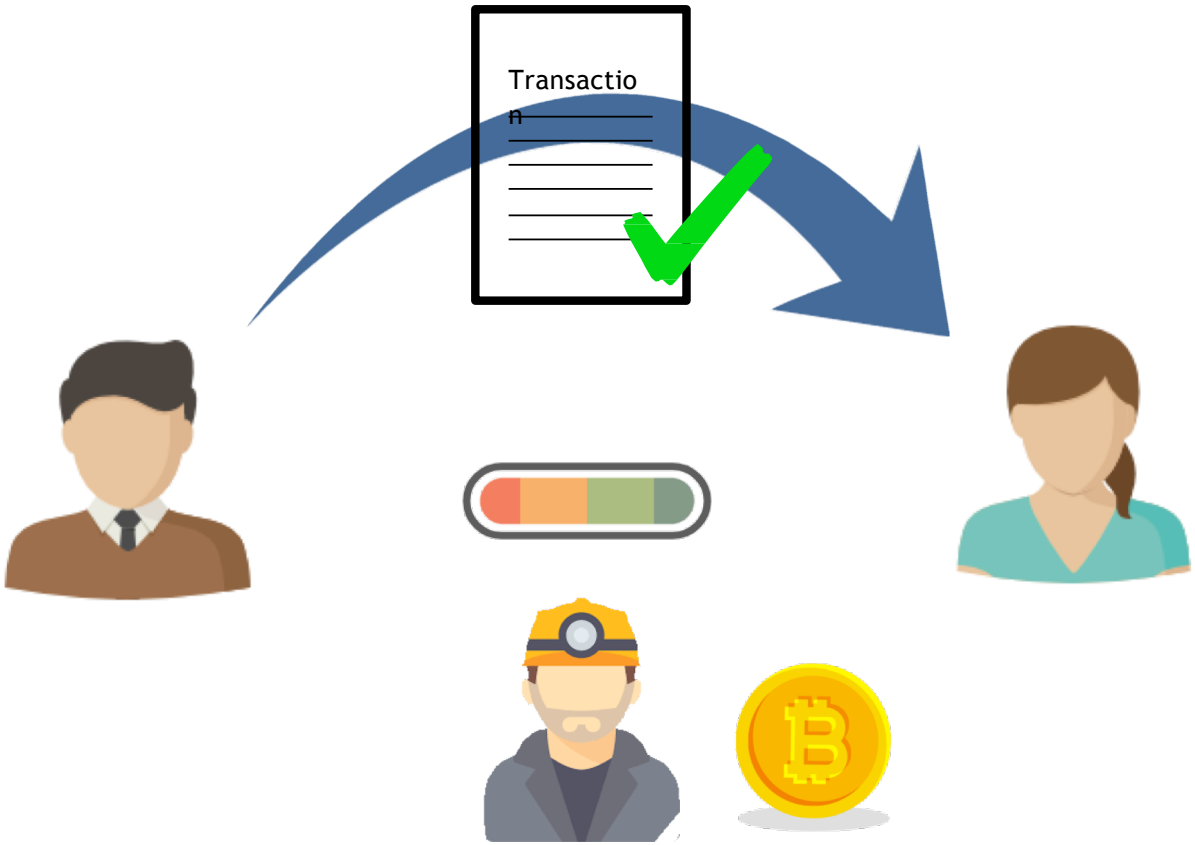
How new data or updates are done on blockchains



"MINING"



Miners are responsible for confirming that transactions on the chain are valid

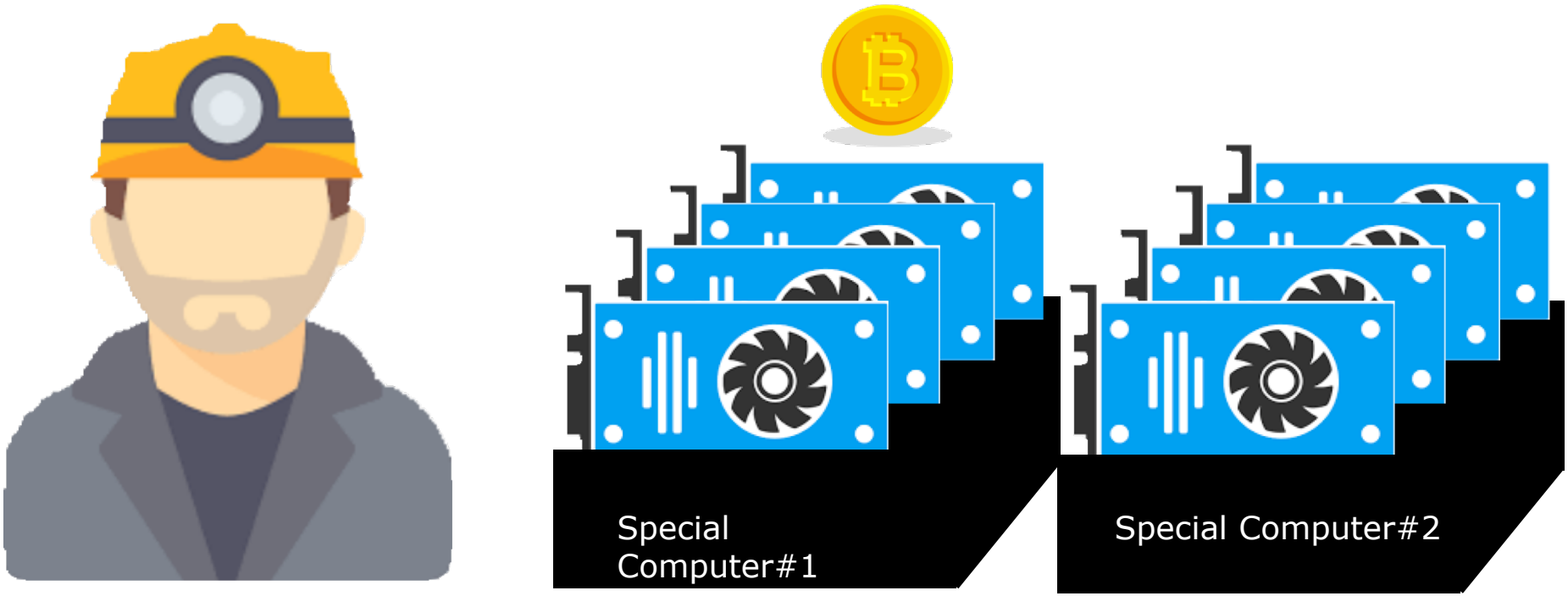


Once the transaction is validated, the miner gets new tokens as a reward

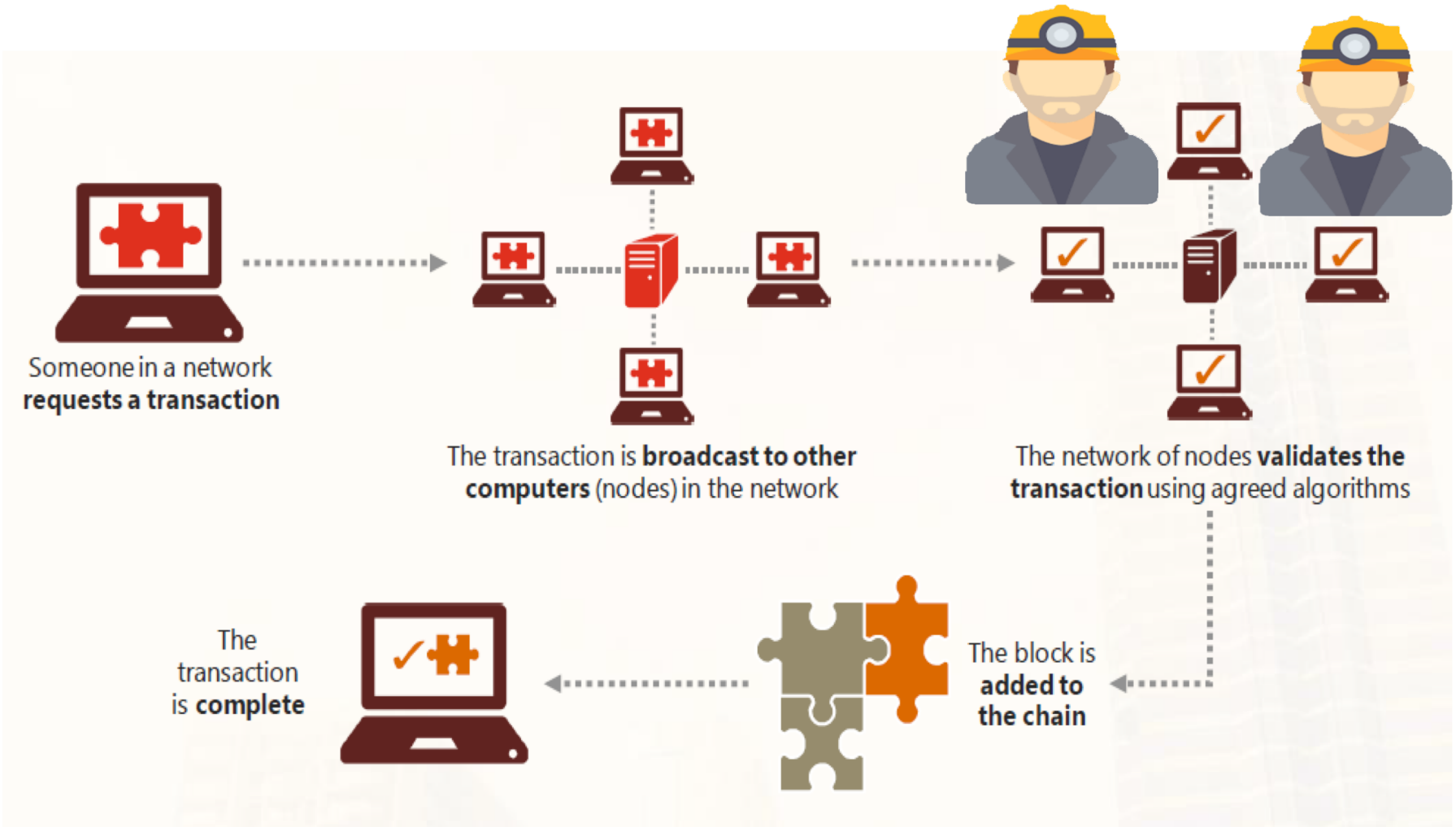
In fact, today there are thousands of miners around the world.

This is important because the more miners or participants in the network, the more secure and resilient it becomes

So how is this done?



Miners use specialised computers called "mining rigs" to validate transactions on the blockchain. Because of the complexity of the mathematical problems, solutions need to be computed by machines.


Someone in a network
requests a transaction
The transaction is **broadcast to other computers** (nodes) in the network
The network of nodes **validates the transaction** using agreed algorithms
The block is **added to the chain**
The transaction is **complete**

Why do we need a blockchain?
Why is it more secure?

We already have processes or entities to do that currently.
Why do we need blockchain? How is it better?

Finance

Banks
Exchanges
Insurance
Venture Cap
Remittance & FX
PayPal

Governance

BSP
Justice System
Land Registry
NSO
BIR
COMELEC

Online

Google
Yahoo
Facebook
Amazon
eBay
LinkedIn

Brokerages

Real Estate
Investment
Trading
Mortgage
Logistics & Customs

Charity & Foundations

PCSO
Non-profits
Donations
Red Cross
Crowdfunding

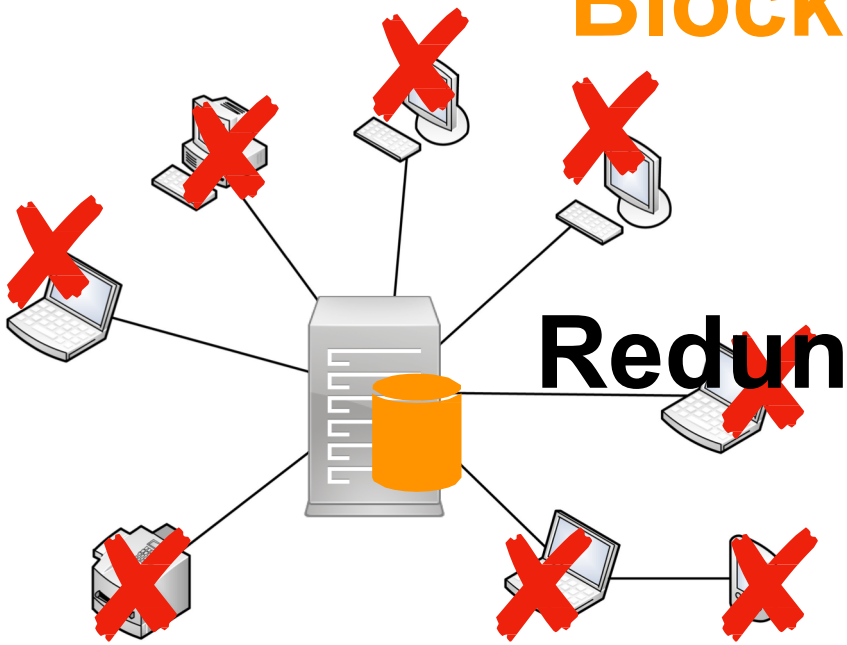
Middlemen or Facilitators

Three Reasons Why Blockchain is More Secure

Blockchain Security

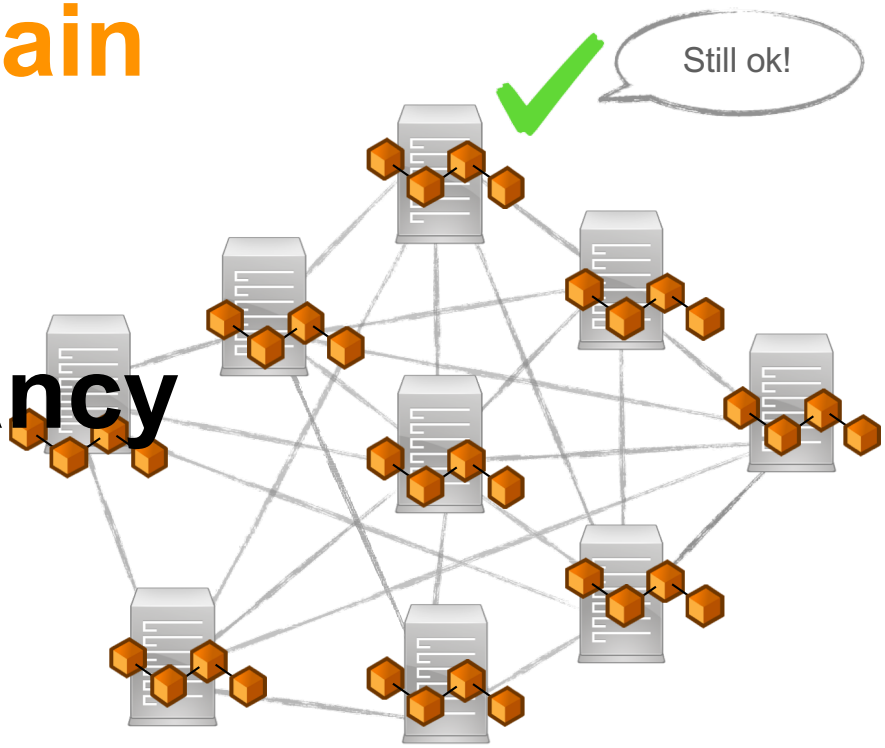
Data is not prone to attack because it is distributed across the network

Database vs Blockchain



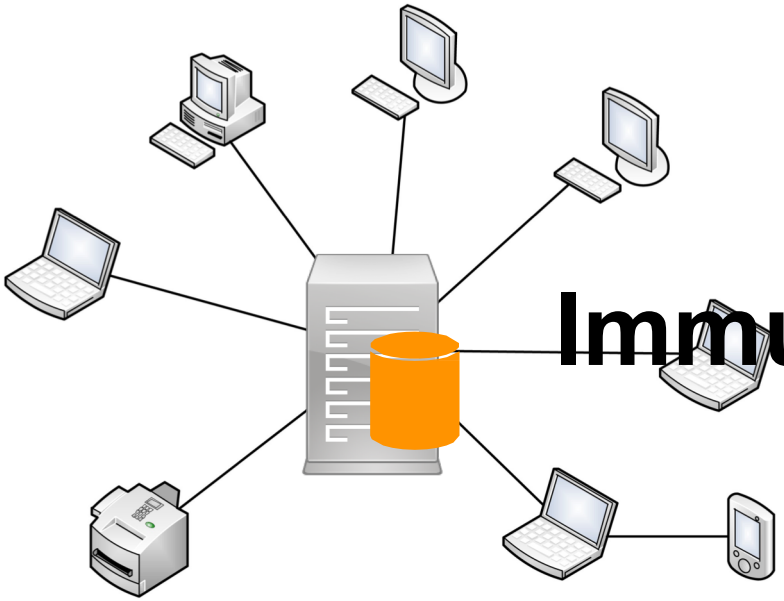
Centralised
Client-Server Network
High systemic risk

Redundancy

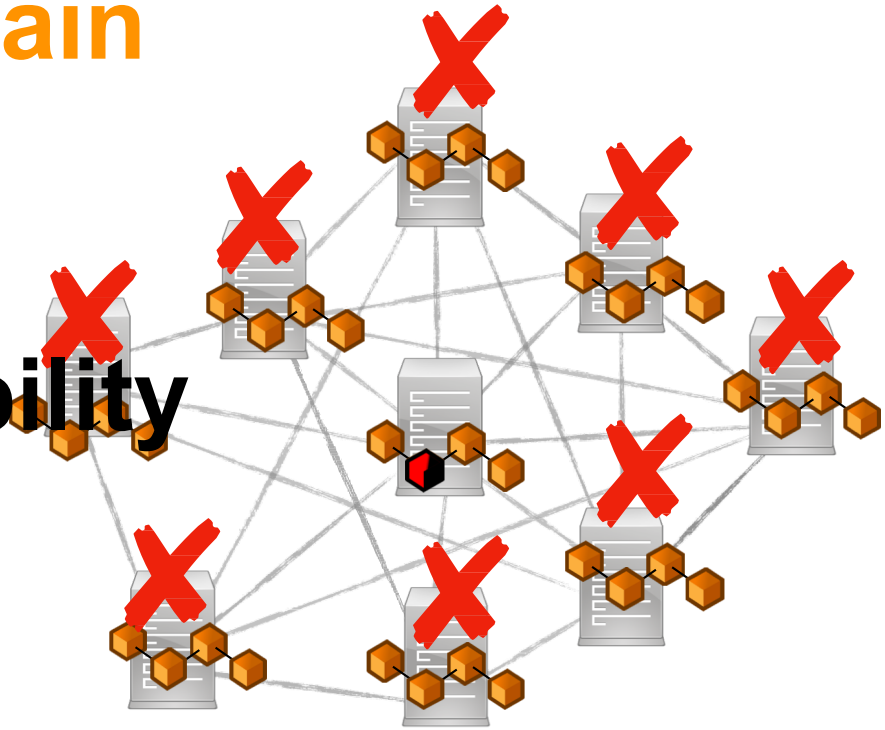


Decentralised
Peer-to-Peer Network
Low systemic risk

Database vs Blockchain



Immutability



Centralised
Client-Server Network
Tamperable, corruptible

Decentralised
Peer-to-Peer Network
Tamper-proof, immutable

Blockchain Security

Data is not prone to attack because it is distributed across the network

Provenance +
Redundancy +
Immutability

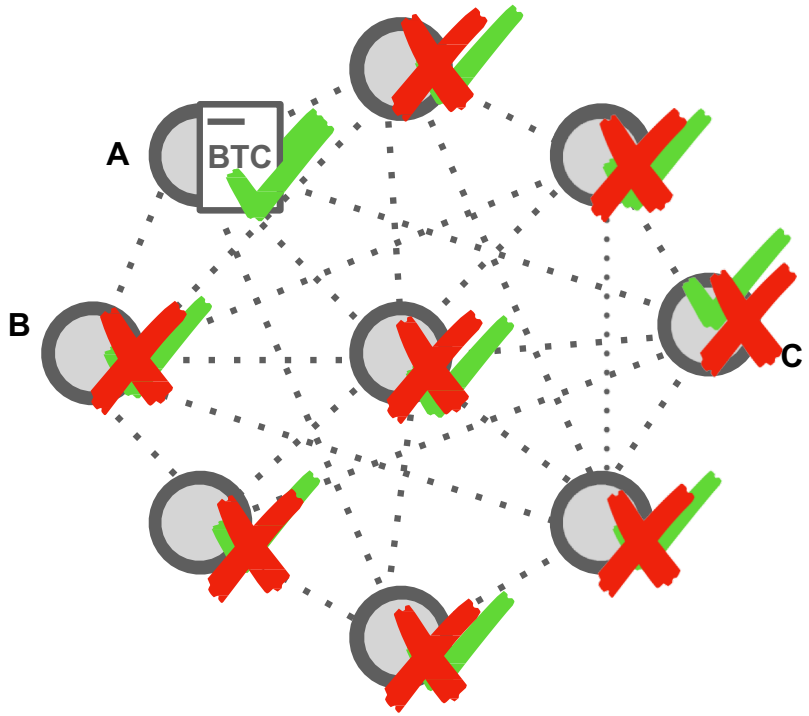
Trust is not required because calculations must be mathematically proven in order to certify that a transaction is legitimate

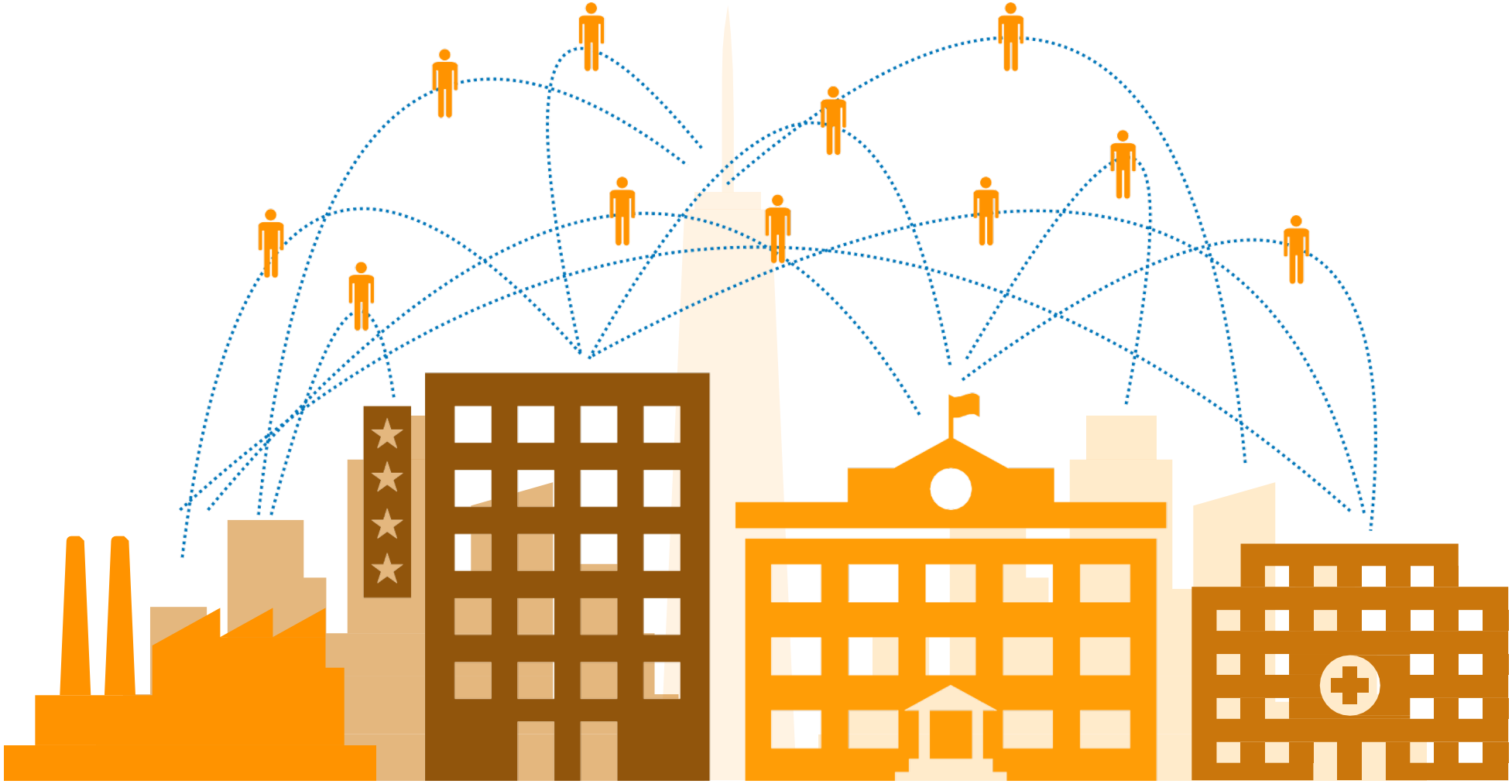
Peer-to-peer Interaction

No more middleman

- Lower cost
- Trust is not required
- Lower risk of fraud
- Lower risk of corruption

Sample Bitcoin Transaction





Blockchain Security

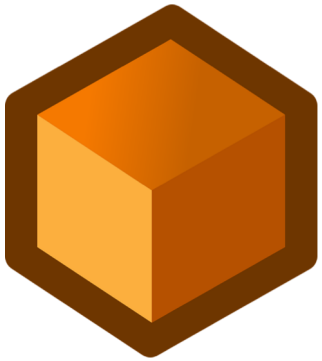
Data is not prone to attack because it is distributed across the network

Trust is not required because calculations must be mathematically proven in order to certify that a transaction is legitimate

Blockchain can be programmed to suit our needs

Endless possibilities

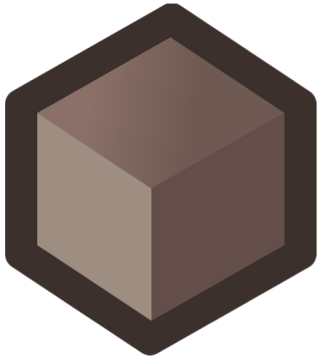
Blockchains are configurable



Public

Anyone can view & update data

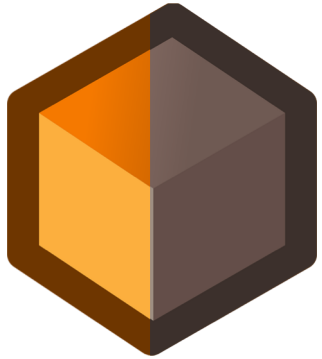
Permission-less



Private

Only select few can view & update data

Permissioned chains



Hybrid

Depending on your role, you can view (partial or all) & update (limited or all)

Use Cases

2008: BITCOIN BLOCKCHAIN

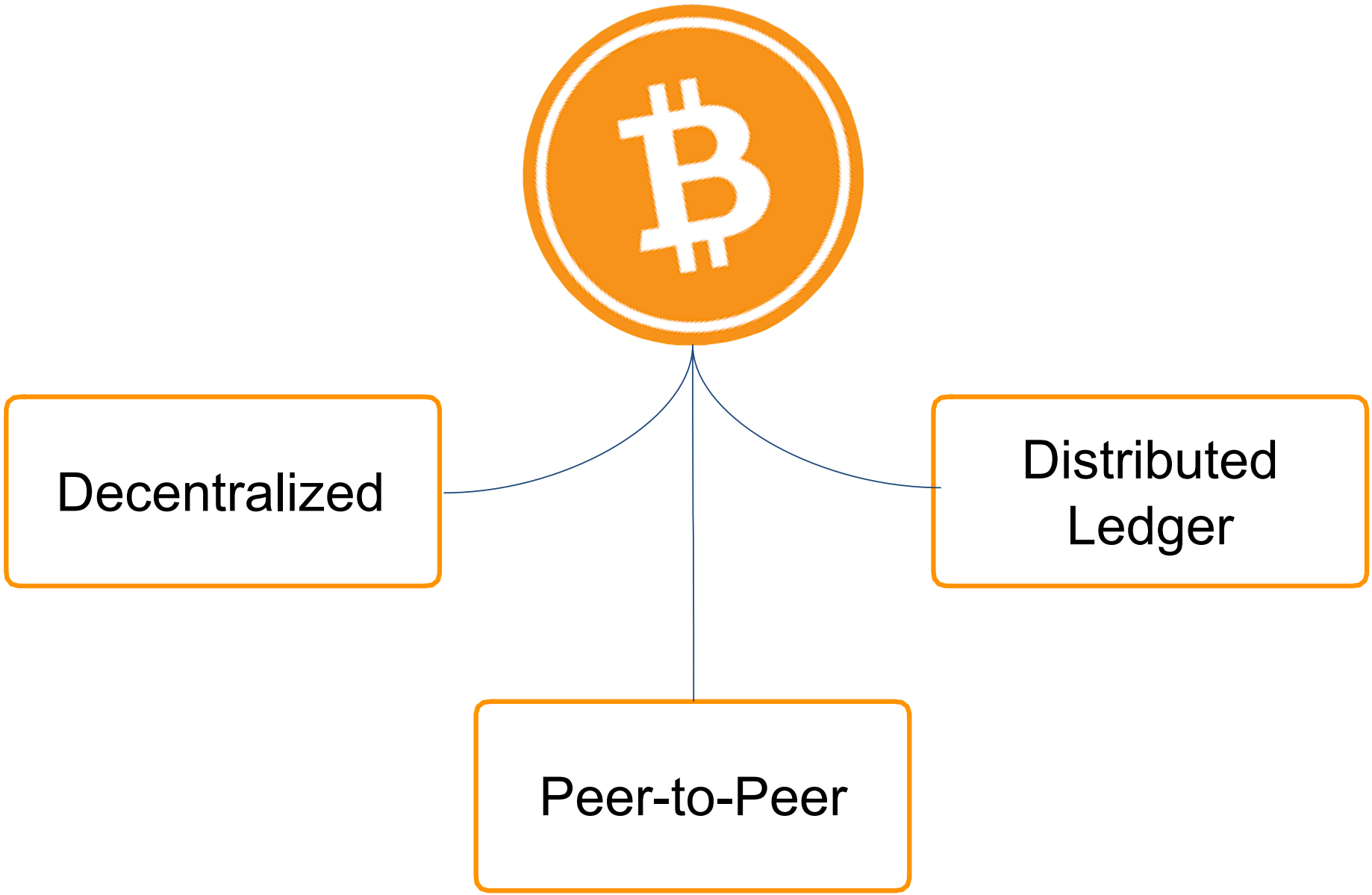
Immutable Ledger

Basic Functions

2014: ETHEREUM BLOCKCHAIN

Smart Contracts

Programmable Blockchain


Decentralized
Distributed Ledger
Peer-to-Peer

contract

/käntrakt/

a written or spoken agreement, especially one concerning employment, sales, or tenancy, that is intended to be enforceable by law.

Smart Contracts

What are smart contracts?

Smart contracts are pieces of code that live on the blockchain and execute commands exactly how they were told to.

Contracts will exist and run as long as the whole network exists.

Should everything be on blockchain?

Can this benefit from decentralization?

Is there a requirement for shared memory?

> A good blockchain application is something that needs decentralization and some kind of shared memory.
>
> Vitalik Buterin, Ethereum Founder

THANK YOU