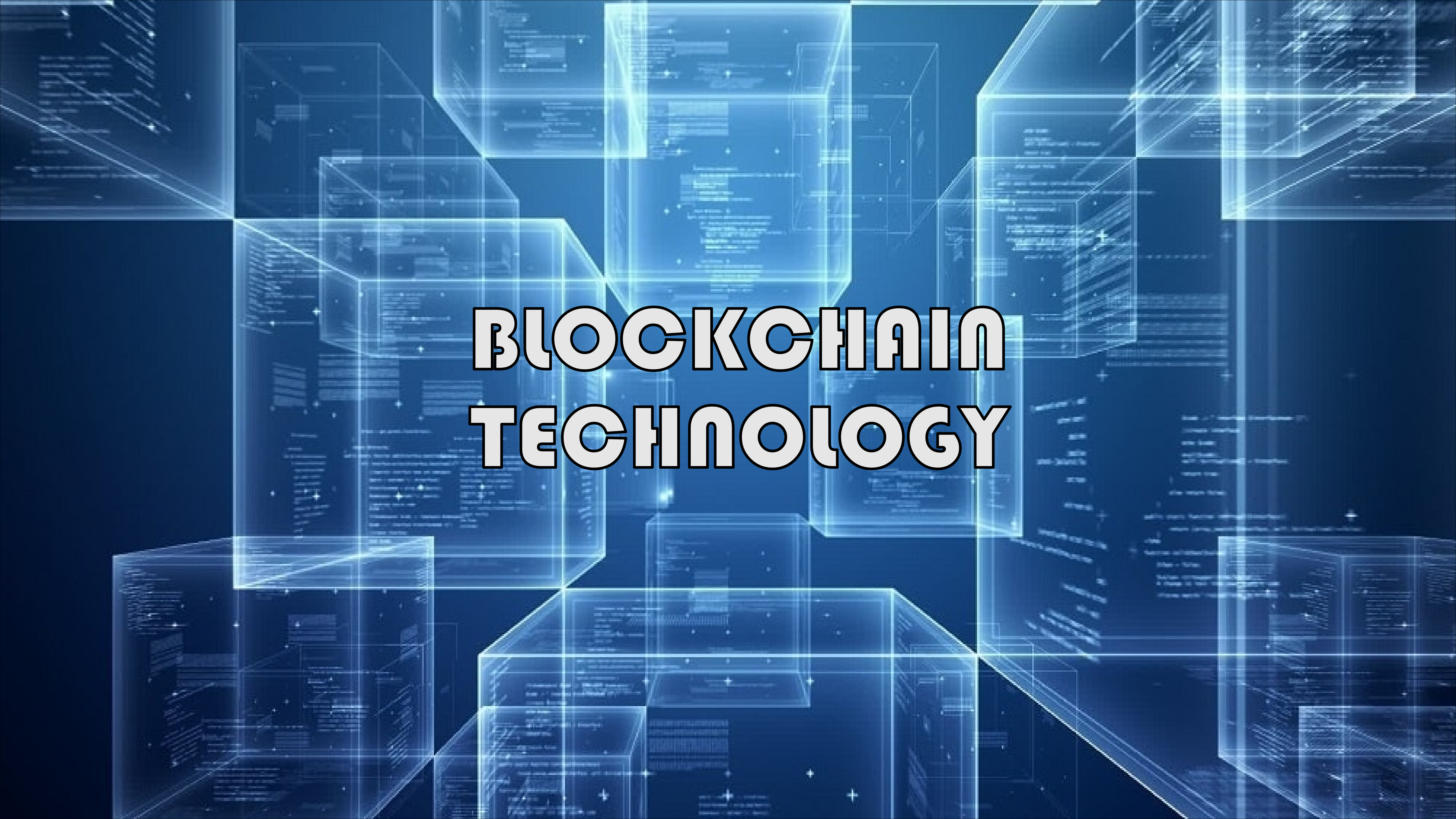


BLOCKCHAIN TECHNOLOGY

> A chain of blocks that contain information.

> Distributed through a peer to peer network
(so anyone can join)

> Created in 1991

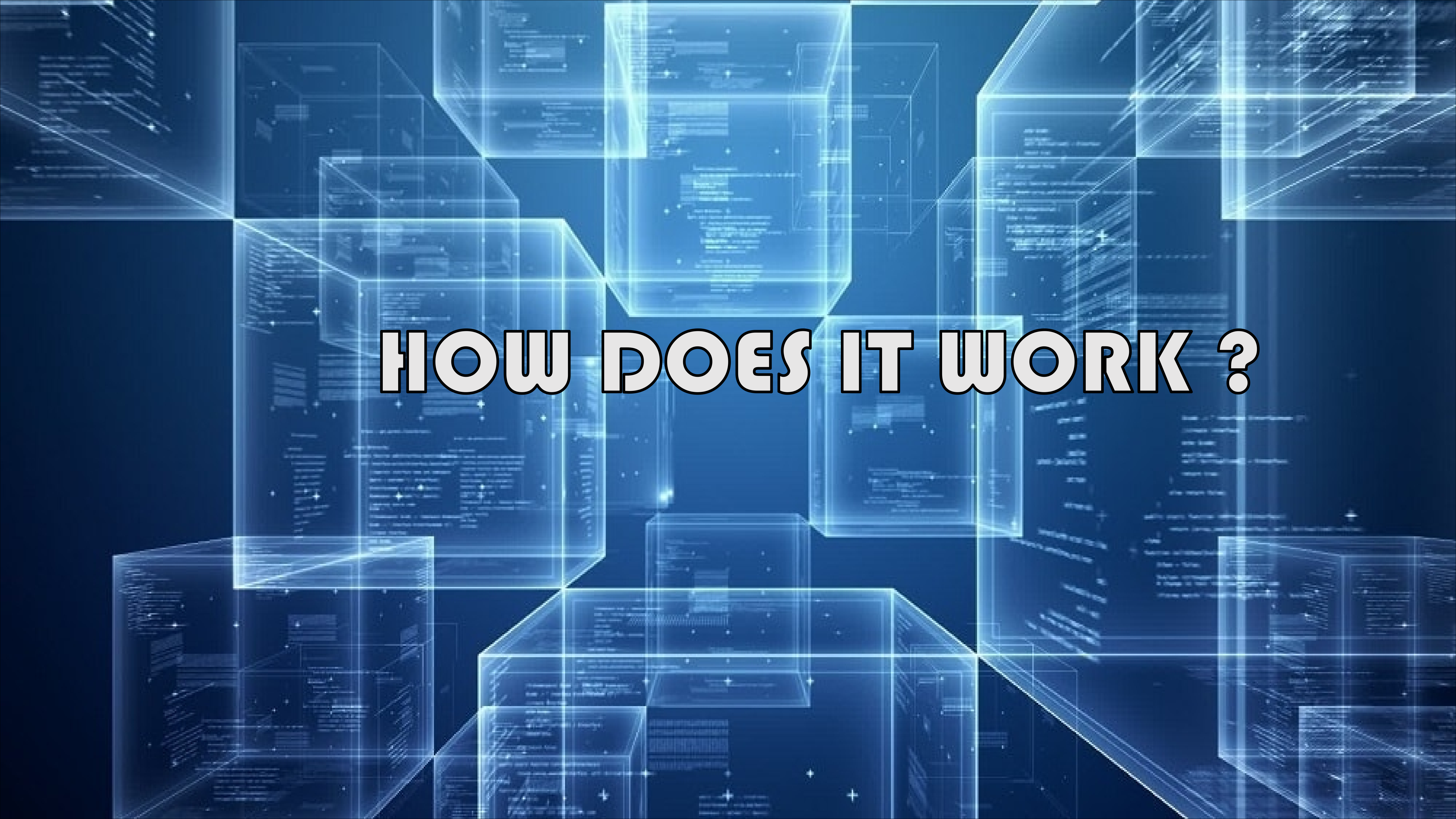
> Originally intended to timestamp digital documents (anti-tempering)

> Made popular by creator(s) of Bitcoin

> Once the data is recorded, it becomes hard to temper with

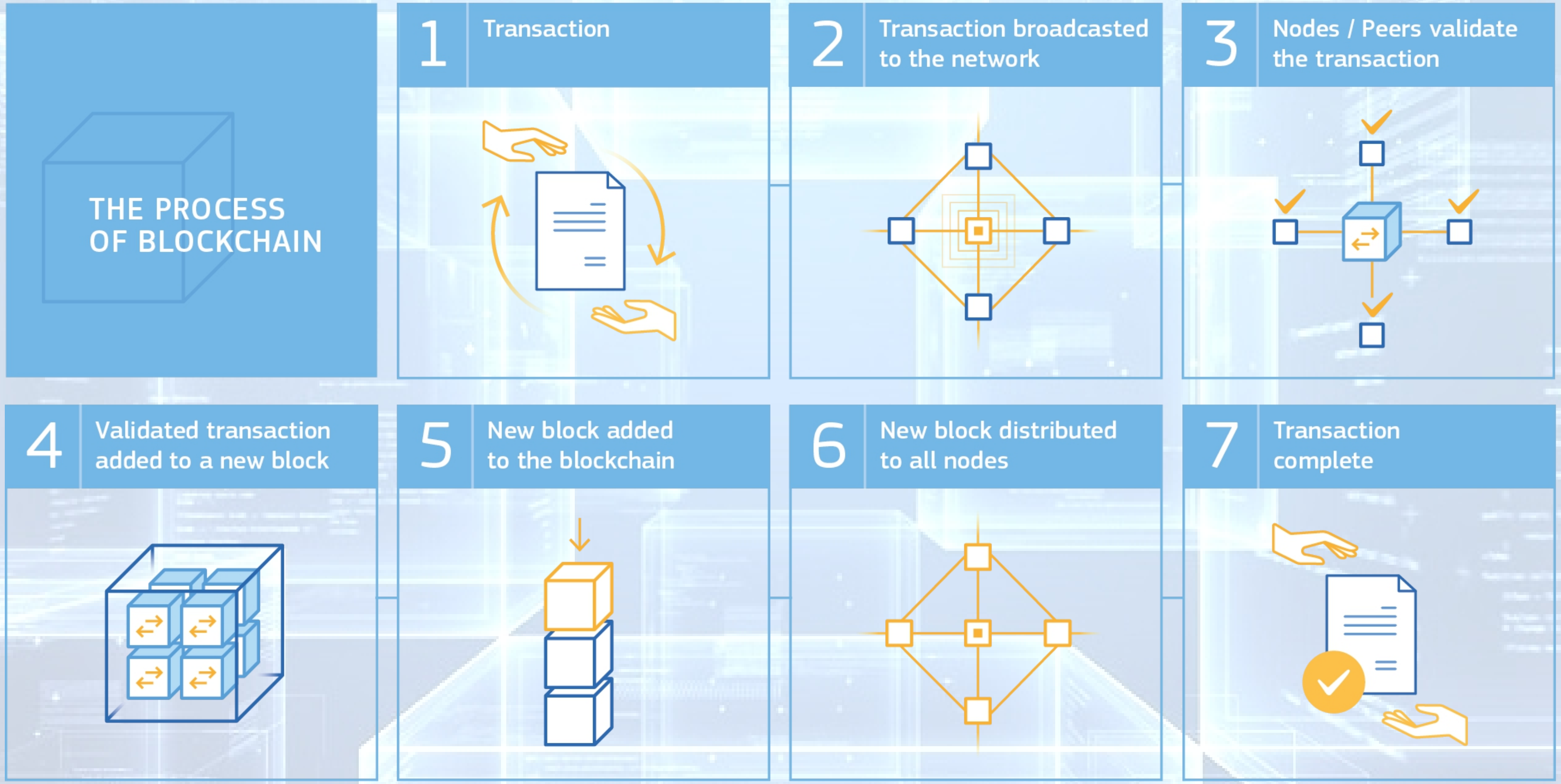
> You can’t change previous blocks

IT’S NOT JUST BITCOIN



HOW DOES IT WORK ?

THE PROCESS OF BLOCKCHAIN



1 Transaction

2 Transaction broadcasted to the network

3 Nodes / Peers validate the transaction

4 Validated transaction added to a new block

5 New block added to the blockchain

6 New block distributed to all nodes

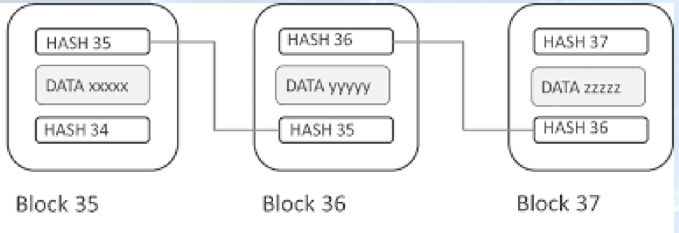
7 Transaction complete

> Each block contains :

- Data
(type depends on type of blockchain)

- Hash *

- Hash of previous block



* Hash :

- fingerprint-

- calculated once created-

- if the block changes, the fingerprint changes -

> If the data of the block changes, the fingerprint changes

> Needs a proof of work before the changes apply
(ie Bitcoin takes 10 minutes before validation)

> Adding one block means all other block also need new proof of work

> Hashing + Proof of work = profit !

Distributed blockchain :

P2P

Every user gets a copy of the blockchain

the node uses this to verify if everything is still in order

> Create a new block

> **Gets send through everyone's block**

> Each block needs proof of work

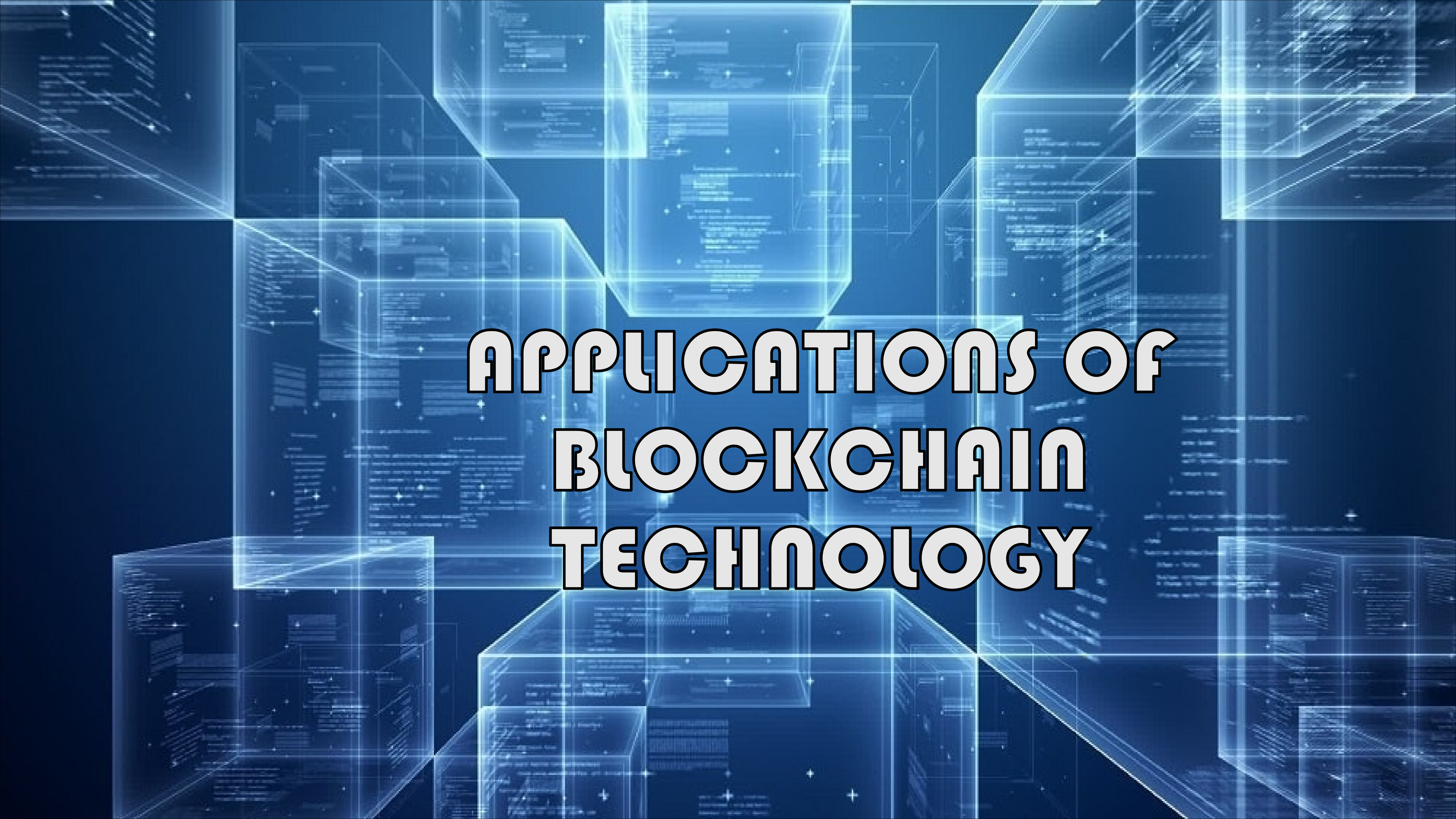
> Node checks every block to validate anti-tempering

> If successfull, the block gets added to the network

> Tempered blocks get rejected by other nodes

> Consensus (valid vs invalid)

> 51% attack



APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

> Cryptocurrency

> Cars : odometer tempering, tracks km’s correctly

> Intellectual properties & pattents

> Notary (stamp.io) not 100% legal

> Digital voting (Swiss company AGORA).

Open Source , not 100% safe (p2p = DDOS & mallware sensitive)

> IBM package tracker WIP

> Collecting royalties for Artists (Imogen Heap)

SMART CONTRACTS

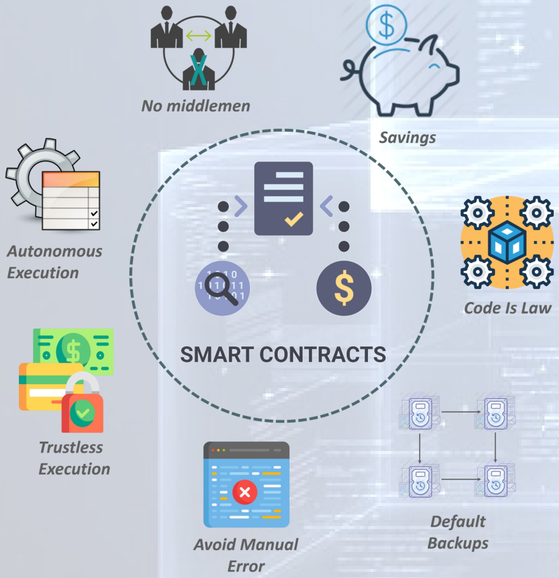
> Simple programs that are stored on the blockchain

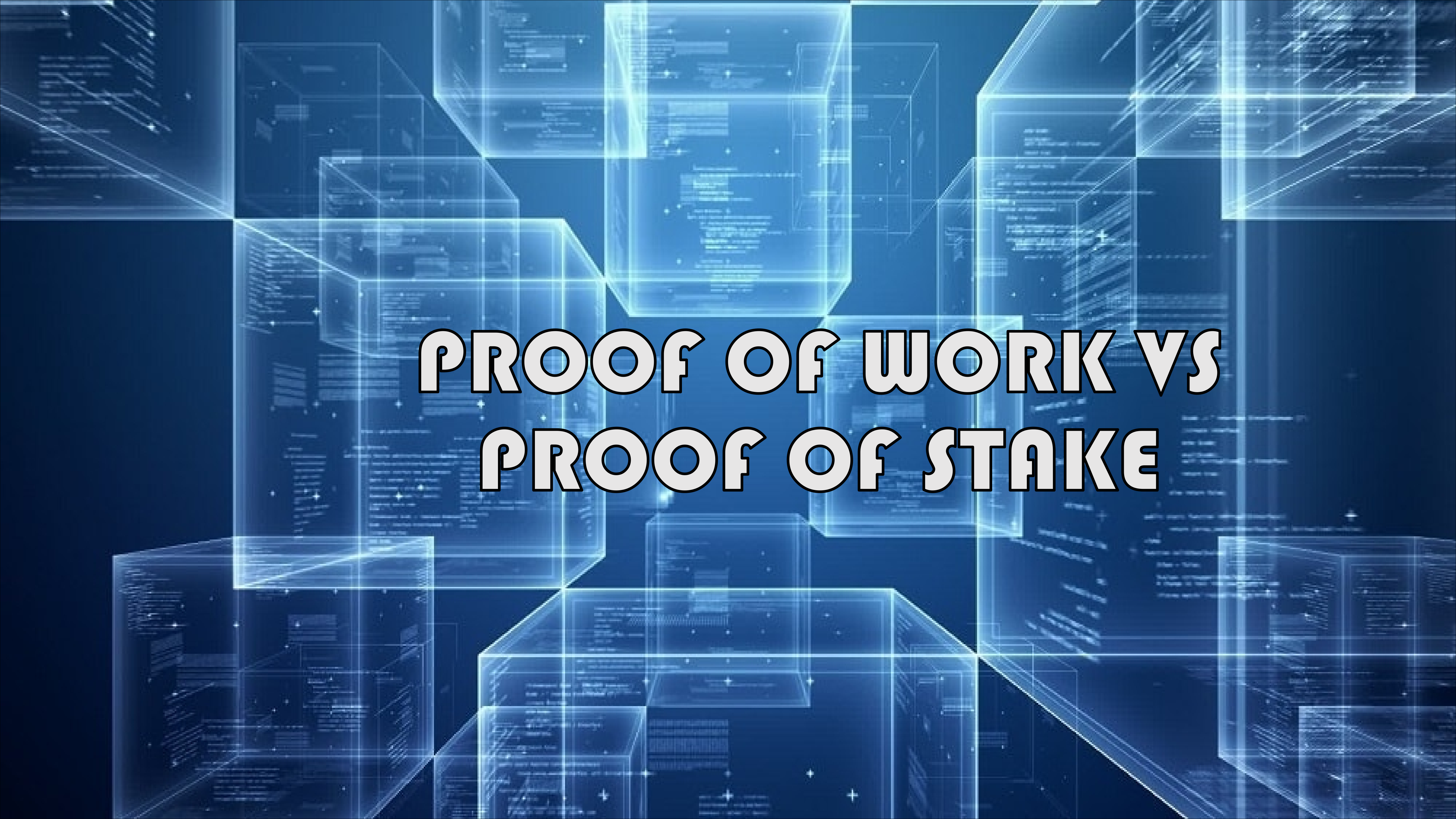
> Can automatically exchange coins, based on certain conditions

> ie. Store medical records for a doctor, but only grand access after digital signature

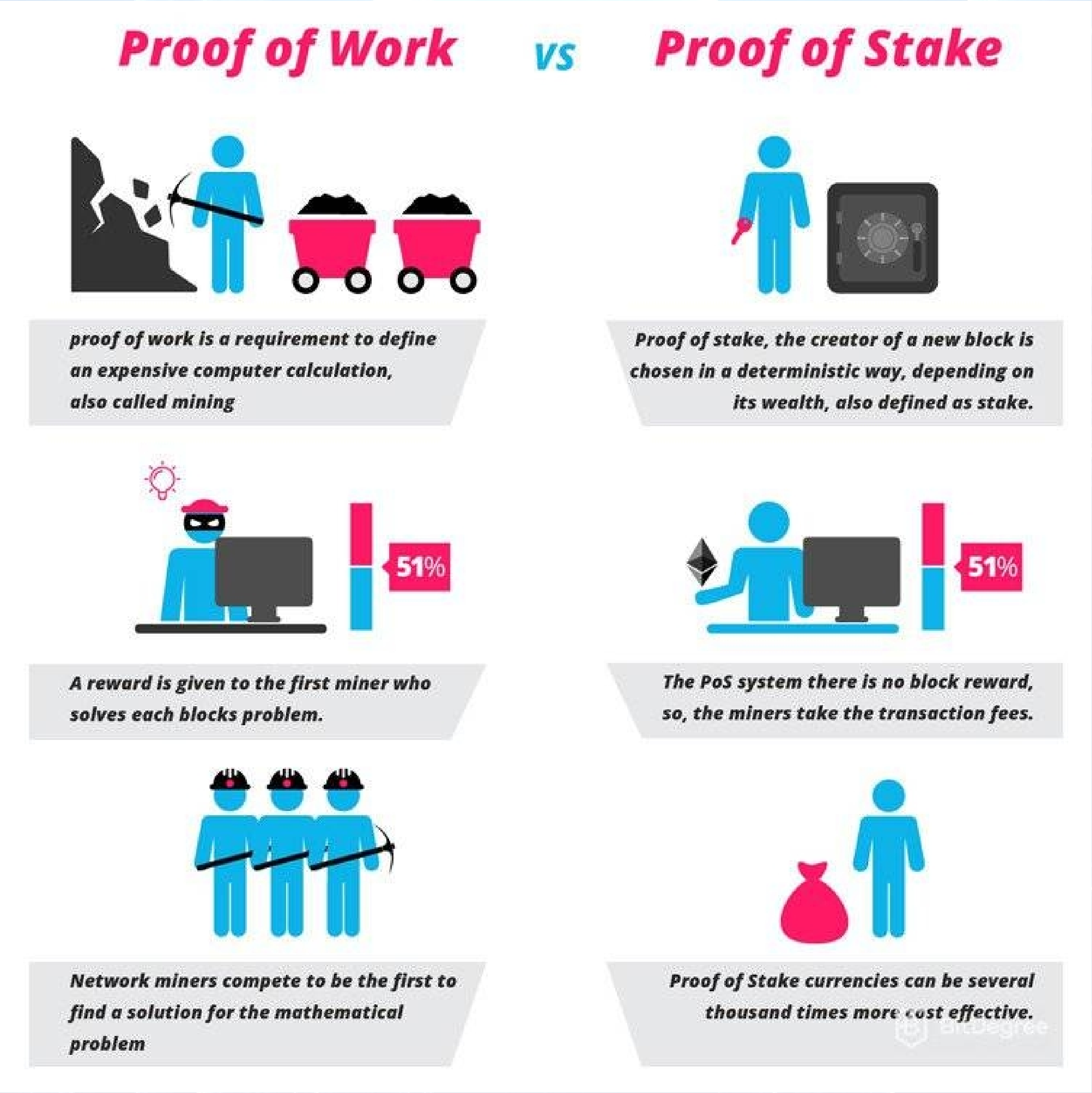
> If successfull, the block gets added to the network

> Tempered blocks get rejected by other nodes





PROOF OF WORK VS PROOF OF STAKE



Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

A reward is given to the first miner who solves each blocks problem.

The PoS system there is no block reward, so, the miners take the transaction fees.

Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

PROOF OF WORK

SHA 265 HASH

> Invented to combat spam emails (‘97)

> Needs huge amounts of electricity

> All nodes have to solve a cryptographic puzzle. Who solves the puzzle first, gets the price. therefore are mines built.

> It gives more rewards to good equipment

> Miners come together in pools

(electricity, fraudulent transactions, more centralized)

> There has to be a better solution

PROOF OF STAKE

> Competition mining is useless

> Validators or Forgers instead of miners

> One node is randomly chosen to validate the next process
= validators .

> Not completely random. Stake to get access .

> The higher the stake, the higher the chance to get chosen
(irl better then going up against mining pools)

> Validators lose proof of stake when validating faulty transactions

PROOF OF STAKE

FAULTY TRANSACTION :

> Stake has to be higher than transaction fees.
If not, faulty transaction

> More decentralised

> Less energy

> Still not perfect

PROOF OF STAKE

> 51% Attack is it’s main weak point

> If next validator doesn’t answer, there is no backup validator

> WIP, less secure then PoW, needs more research

> Less energy

> Still not perfect

IN CONCLUSION

> Needs more time

> Interesting evolution

> It’s impact is getting bigger and bigger

> Answer to inequality

> Put land property on it

> Peers come together and share wealth

><

DEMO

ON

HASHING

PRINCIPAL