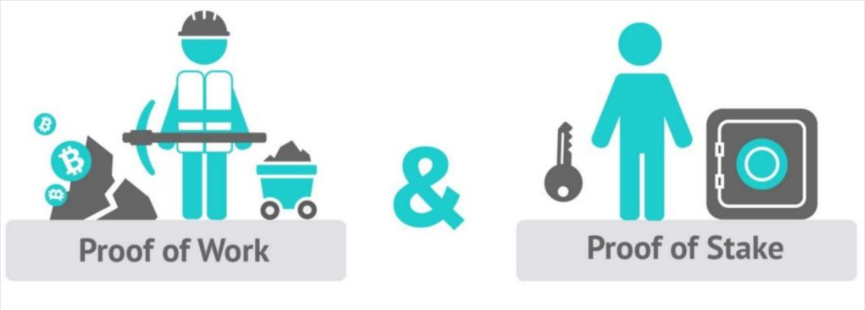
# BLOCKCHAIN FOR DUMMIES

Vuong Huynh
SAM Miracle

# CONTENTS



WHAT IS BLOCKCHAIN

PROOF-OF-STAKE AND PROOF-OF-WORK

SMART CONTRACT

# WHAT IS BLOCKCHAIN?

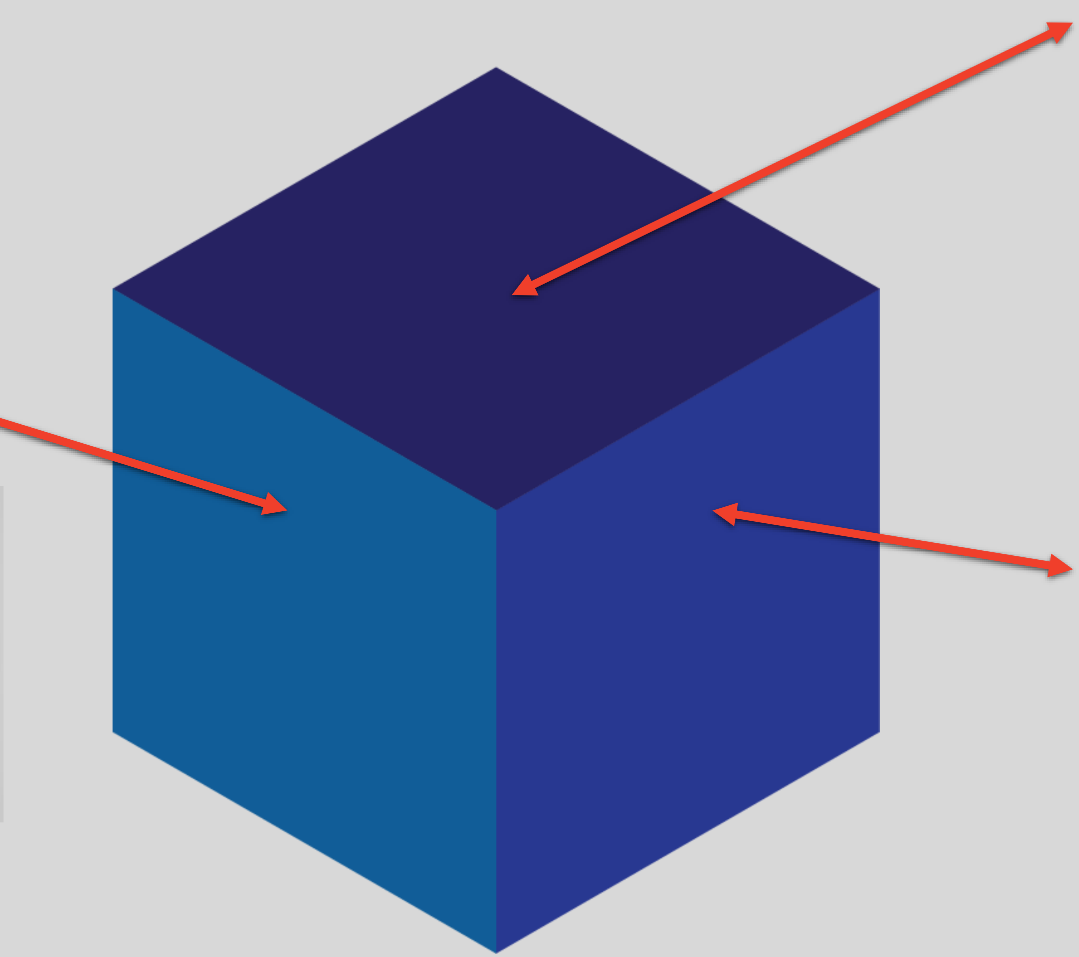
What is this, how it work on basic level and what problems it solves ?

It’s super easy, trust me!

# WHAT IS BLOCKCHAIN

- A blockchain is a chain of blocks that contains information.
- Was originally described in 1997, intended to timestamp digital documents to prevent backdating them or to tamper with them.
- Was adopted by Satoshi Nakamoto in 2009 to create Bitcoin.
- A blockchain is a Distributed ledger, completely open to everyone.
- It's very difficult or almost impossible to change the data that had been recorded inside a blockchain.

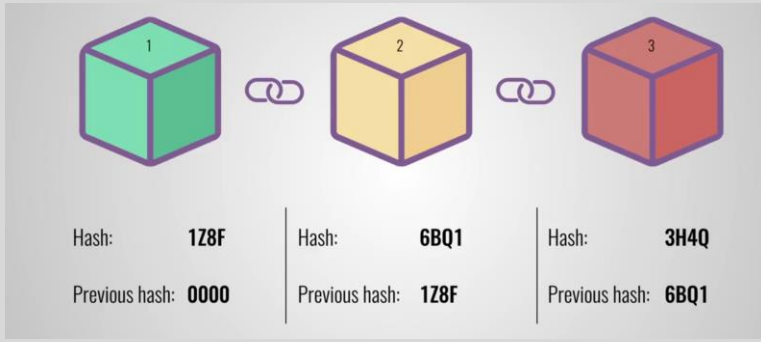
# WHAT IS BLOCKCHAIN



**Data**

From address: **a**
To address: **b**
Amount: **20 token**

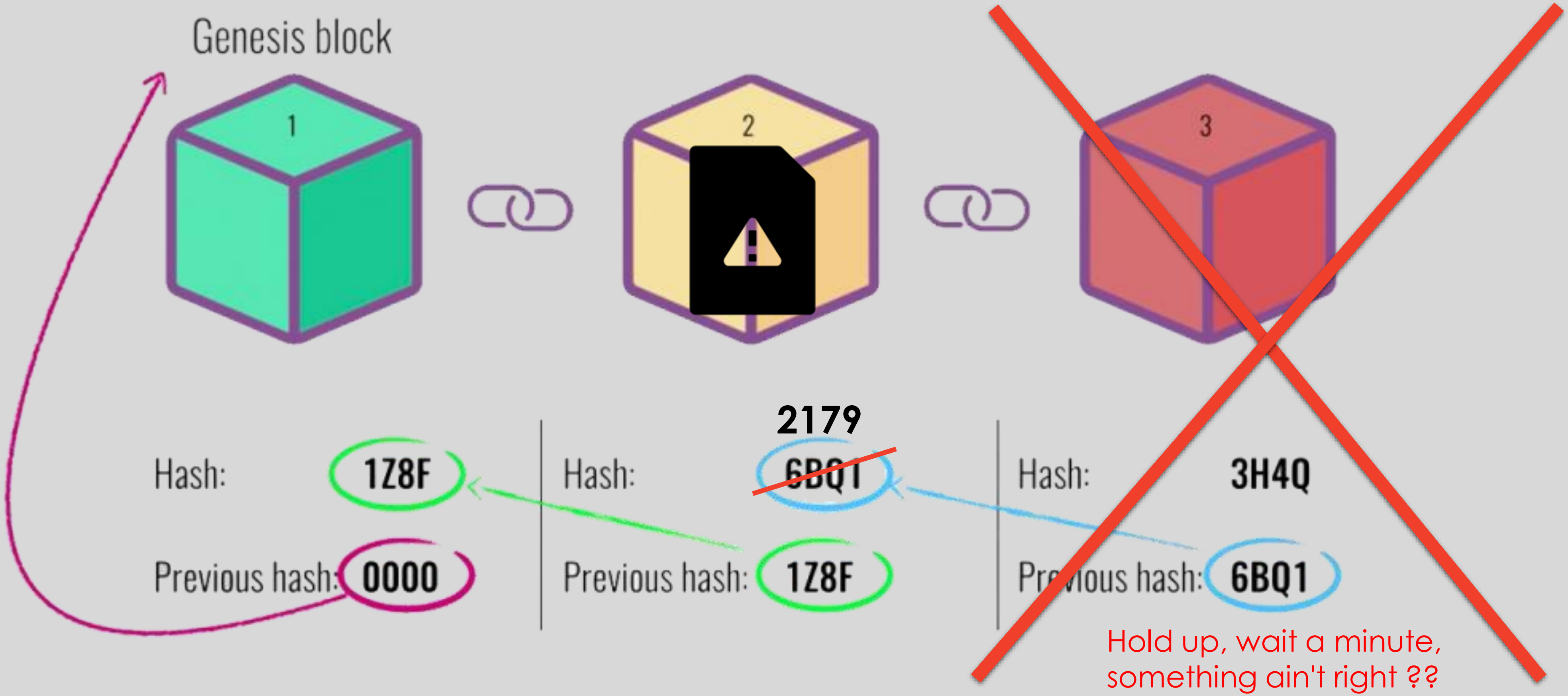
**Hash of previous block**



| | | | | | |
|---|---|---|---|---|---|
| Hash: | 1Z8F | Hash: | 6BQ1 | Hash: | 3H4Q |
| Previous hash: | 0000 | Previous hash: | 1Z8F | Previous hash: | 6BQ1 |

**Hash**
e12309bb4wi833db

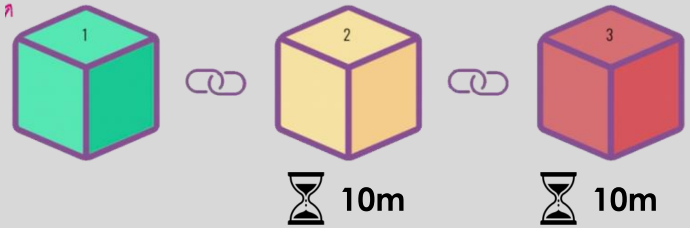
# WHAT IS BLOCKCHAIN



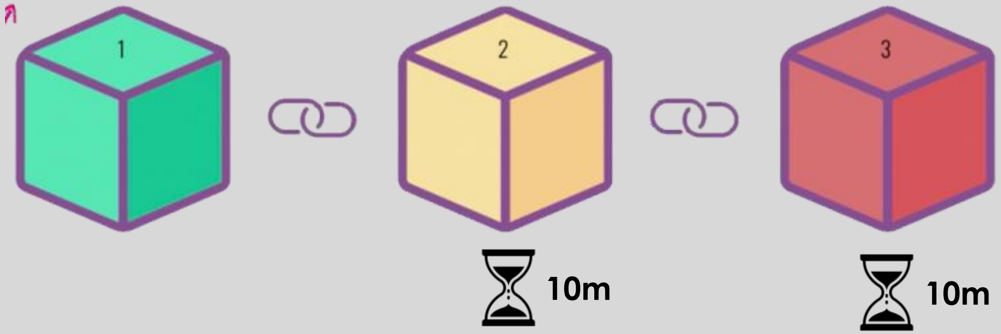
Hold up, wait a minute, something ain't right ??

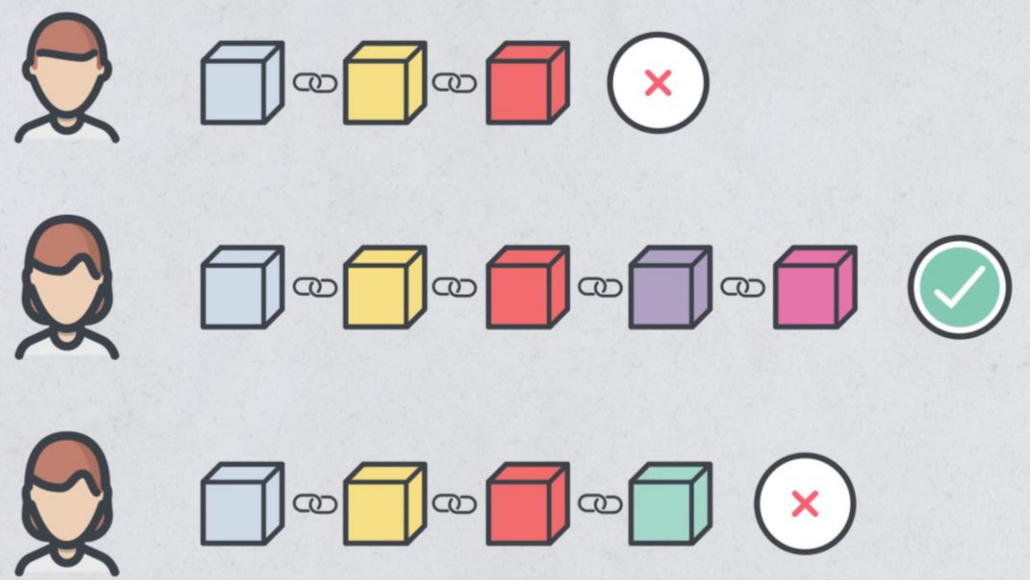
# PROOF – OF – WORK

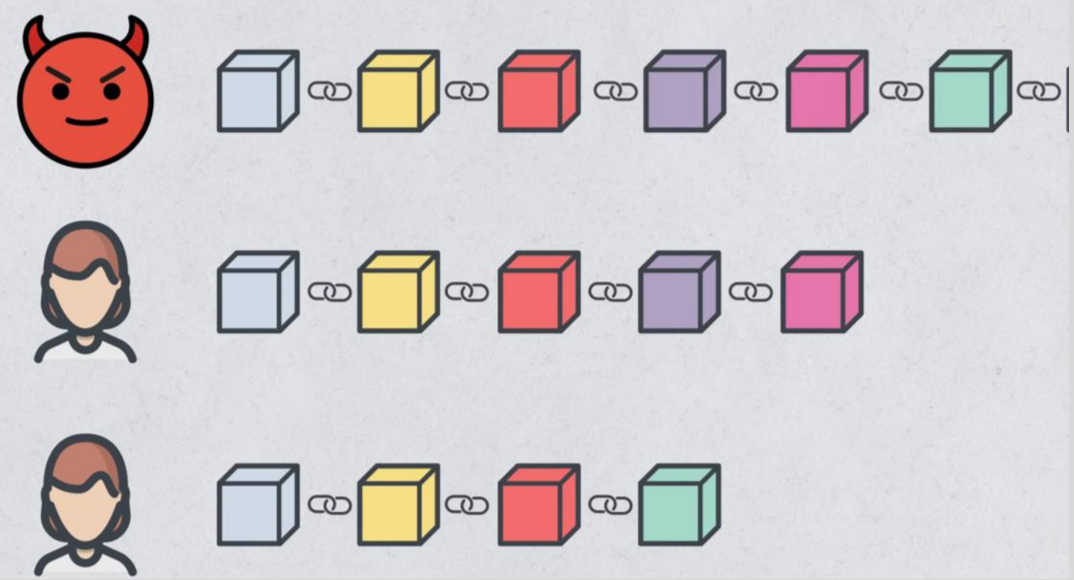
- First introduced in 1994 to combat spam emails, used by Satoshi Nakamoto when he created Bitcoin in 2009.
- Decentralized consensus mechanism that requires nodes of a network to expend effort solving a cryptographic puzzle.
- Use to slow down the creation of new blocks & secure the network.
- Make it very hard to tamper with blocks.



# NETWORK DIFFICULTY



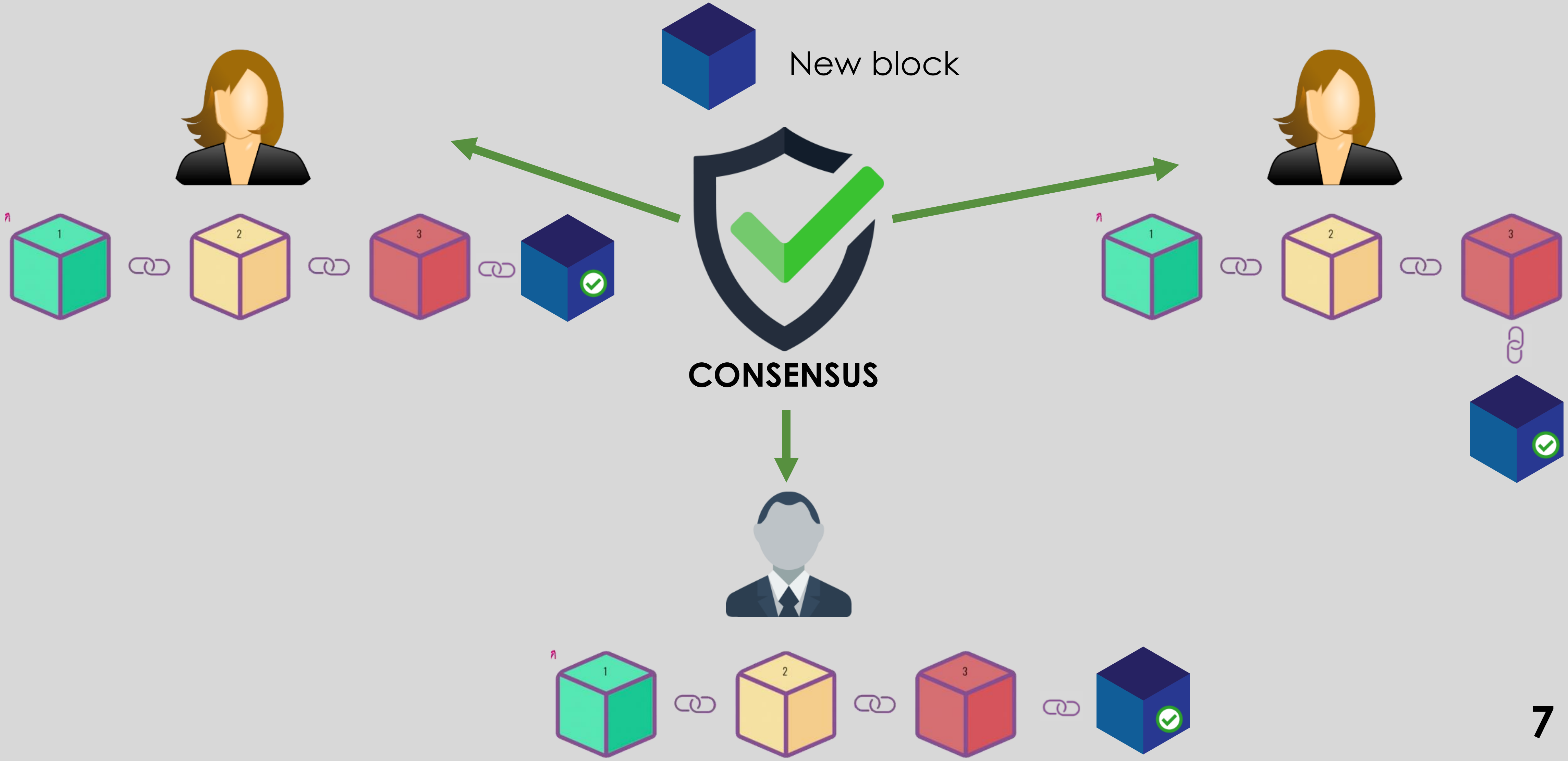




# DISTRIBUTED AND PEER-TO-PEER NETWORK

P2P Network
(Torrent is an example)

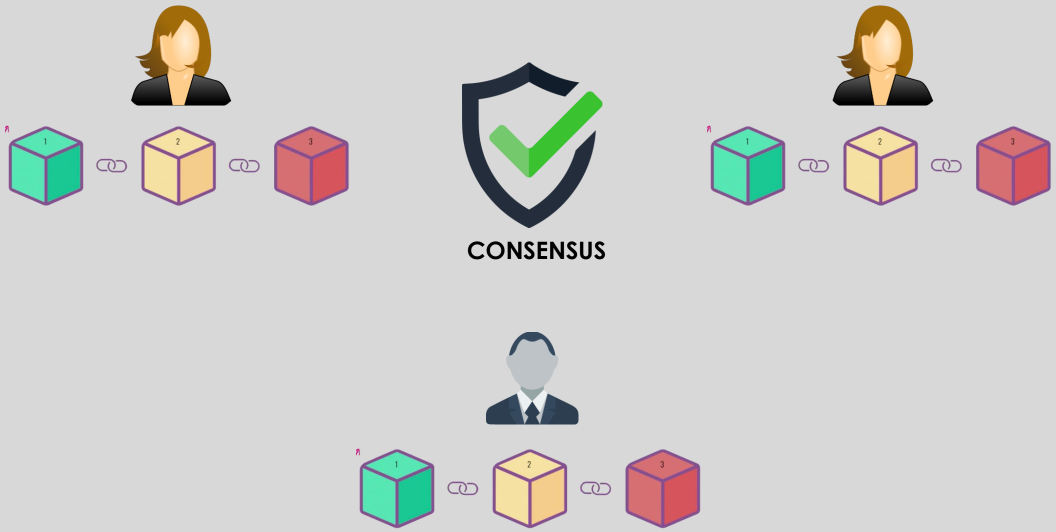
# DISTRIBUTED AND PEER-TO-PEER NETWORK



New block

CONSENSUS

# DISTRIBUTED AND PEER-TO-PEER NETWORK



- All the nodes in the network create consensus.
- They agree about what blocks are valid and which are not.
- Block that're tampered will be rejected by other nodes.
- If some-one want to successfully tamper with a blockchain:
  - Tamper with all blocks in the chain.
  - Redo the PoW for each blocks.
  - Take control more than 50% of the P2P.

IMPOSSIBLE

# PRACTICAL APPLICATION

Medical record

E-Notary

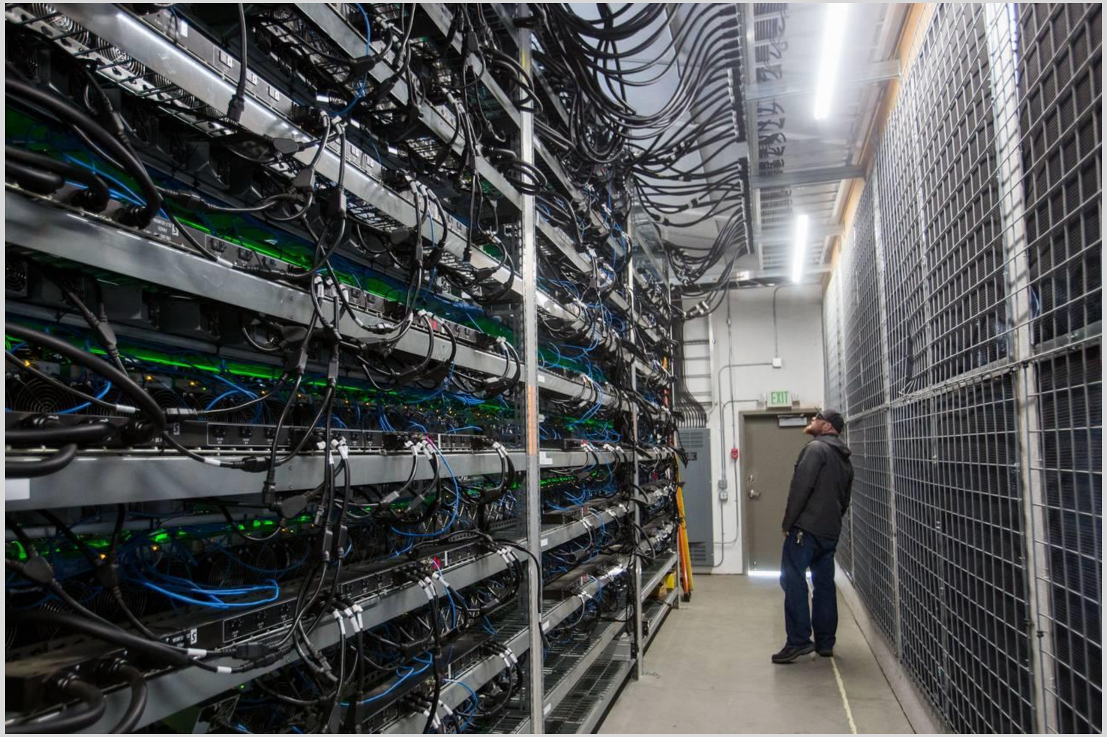
Taxes collection

# PROOF-OF-STAKE
AND
# PROOF-OF-WORK

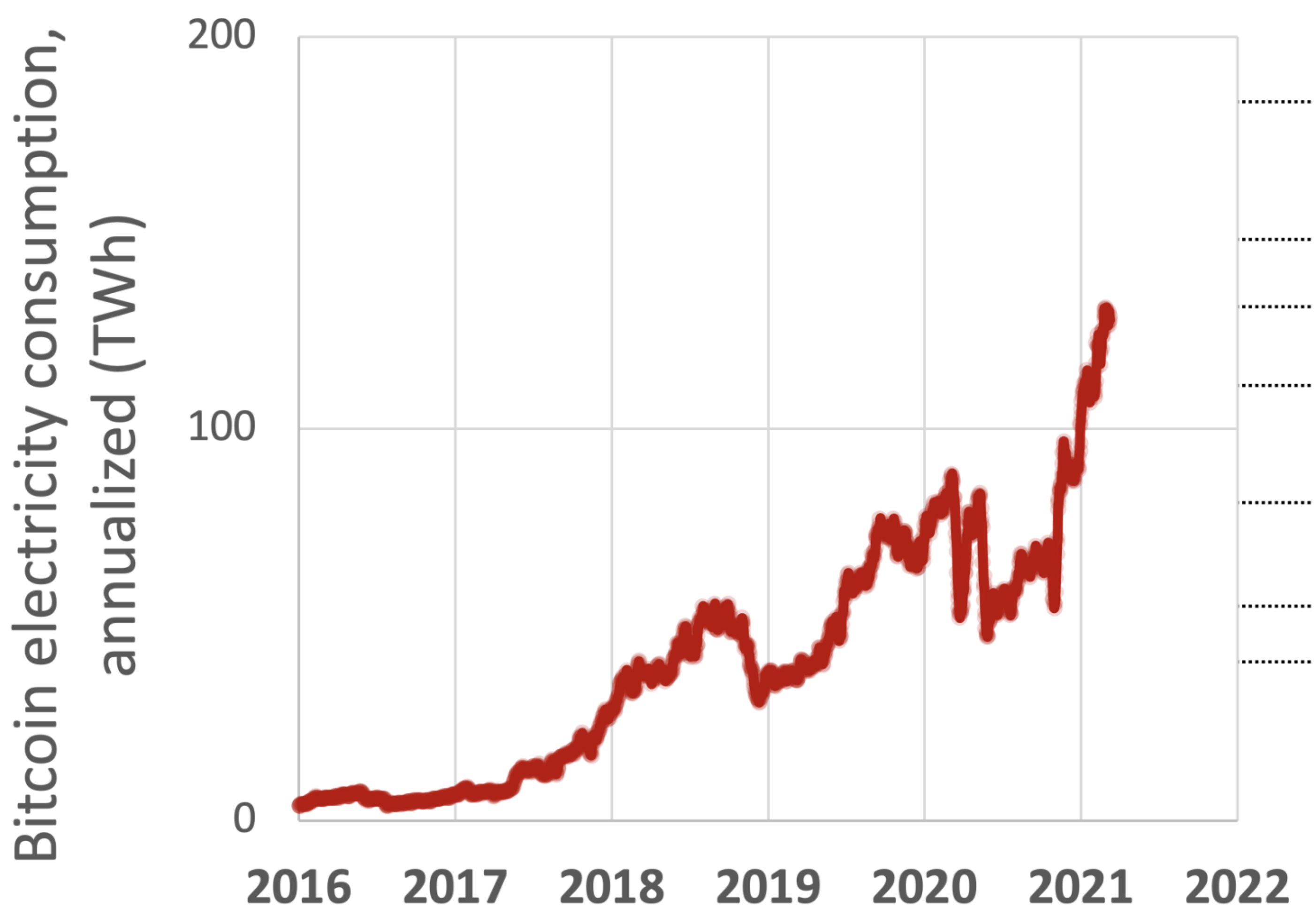
We'll research about Proof-of-Stake, deep dive into proof-of-work,
and find out what is the difference between them

# INADEQUACIES OF PROOF-OF-WORK

- The puzzle solve by Miner and the first one find the solution get the miner reward → People start to build larger and larger mining farm
- The Bitcoin Network is 80.704.000 PetaFLOPS (2018)
- World most powerful supercomputer (Fugaku) is 442.01 PetaFLOPS



# INADEQUACIES OF PROOF-OF-WORK



<u>**Country equivalent:**</u>

**Thailand:** 185 TWh

**Egypt:** 151 TWh

**Sweden:** 131 TWh

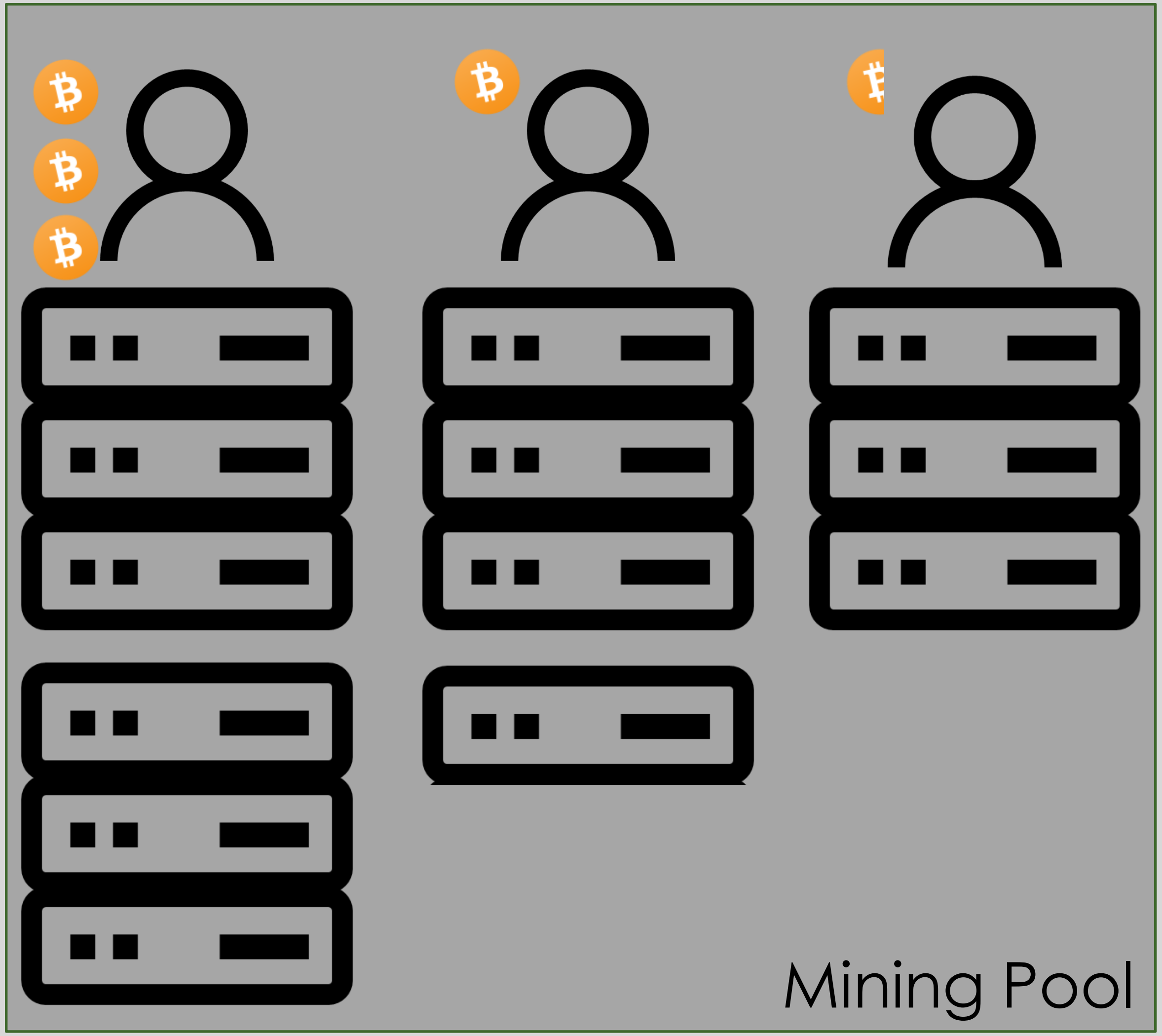
**Netherlands:** 111 TWh

**Belgium:** 82 TWh

**Israel:** 56 TWh

**New Zealand:** 41 TWh

# INADEQUACIES OF PROOF-OF-WORK



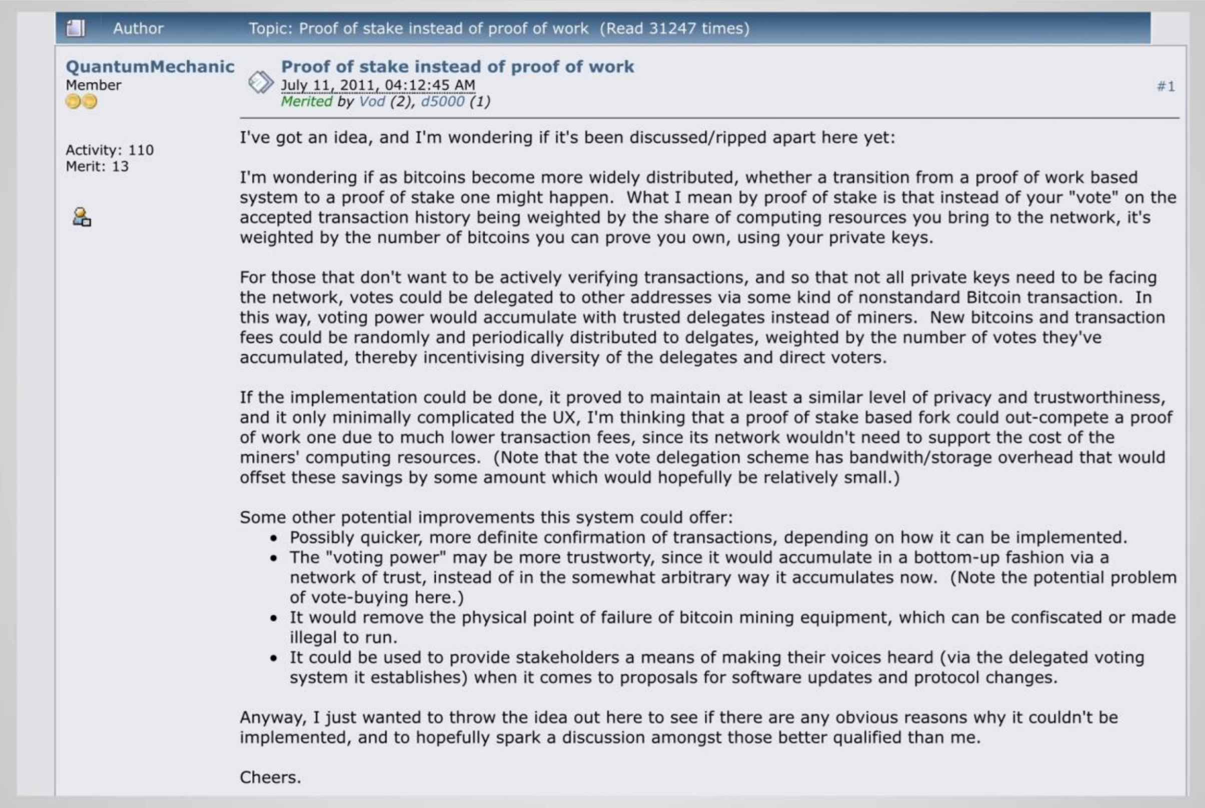
- Give more reward for people with better and more equipment.
- The higher hashrate is, the higher you’ll get chance to create a new block and receive the mining reward.
- The miners combine their hashing power and distribute the reward evenly across everyone → Mining pool.

# INADEQUACIES OF PROOF-OF-WORK

- Huge amount of energy usage.
- Mining pool → Centralization.

→ WE NEED A NEW ALGORITHM!

# PROOF-OF-STAKE



Author | Topic: Proof of stake instead of proof of work (Read 31247 times)

**QuantumMechanic**
Member

Activity: 110
Merit: 13

**Proof of stake instead of proof of work**
July 11, 2011, 04:12:45 AM
Merited by Vod (2), d5000 (1)

#1

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys.

For those that don't want to be actively verifying transactions, and so that not all private keys need to be facing the network, votes could be delegated to other addresses via some kind of nonstandard Bitcoin transaction. In this way, voting power would accumulate with trusted delegates instead of miners. New bitcoins and transaction fees could be randomly and periodically distributed to delgates, weighted by the number of votes they've accumulated, thereby incentivising diversity of the delegates and direct voters.

If the implementation could be done, it proved to maintain at least a similar level of privacy and trustworthiness, and it only minimally complicated the UX, I'm thinking that a proof of stake based fork could out-compete a proof of work one due to much lower transaction fees, since its network wouldn't need to support the cost of the miners' computing resources. (Note that the vote delegation scheme has bandwith/storage overhead that would offset these savings by some amount which would hopefully be relatively small.)

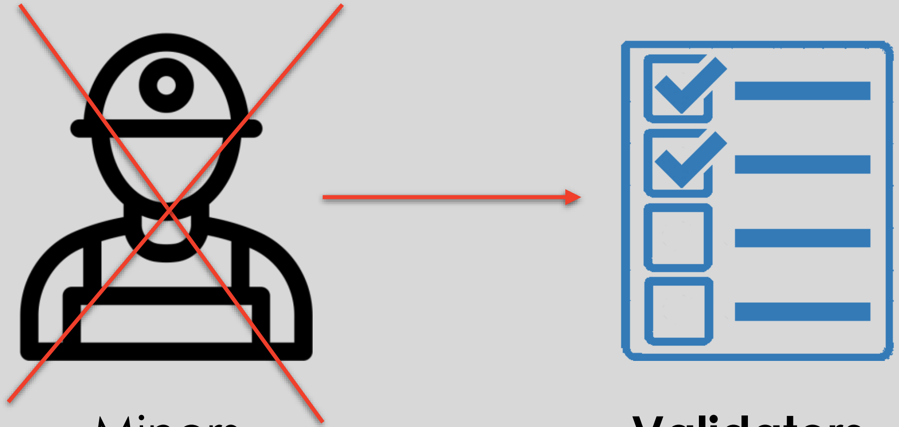
Some other potential improvements this system could offer:

- Possibly quicker, more definite confirmation of transactions, depending on how it can be implemented.
- The "voting power" may be more trustworty, since it would accumulate in a bottom-up fashion via a network of trust, instead of in the somewhat arbitrary way it accumulates now. (Note the potential problem of vote-buying here.)
- It would remove the physical point of failure of bitcoin mining equipment, which can be confiscated or made illegal to run.
- It could be used to provide stakeholders a means of making their voices heard (via the delegated voting system it establishes) when it comes to proposals for software updates and protocol changes.

Anyway, I just wanted to throw the idea out here to see if there are any obvious reasons why it couldn't be implemented, and to hopefully spark a discussion amongst those better qualified than me.

Cheers.

- Proposed by QuantumMechanic in 2011
- The basic idea is using an election process in which one node is randomly choose to validate the next block.

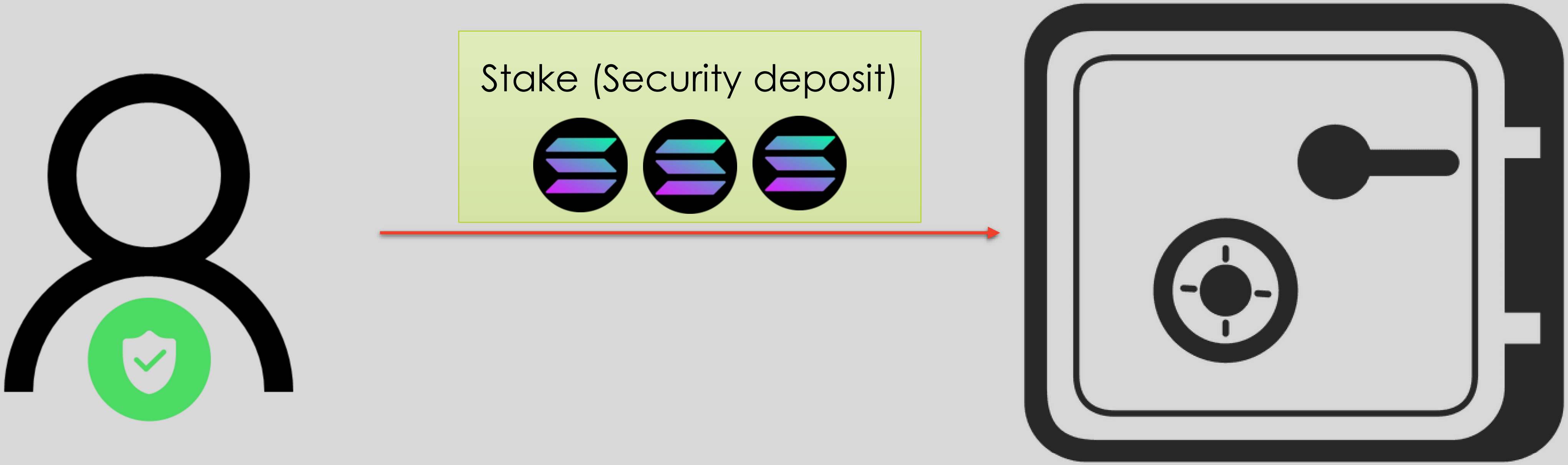


Miners

**Validators**

**Mint (forge) blocks**

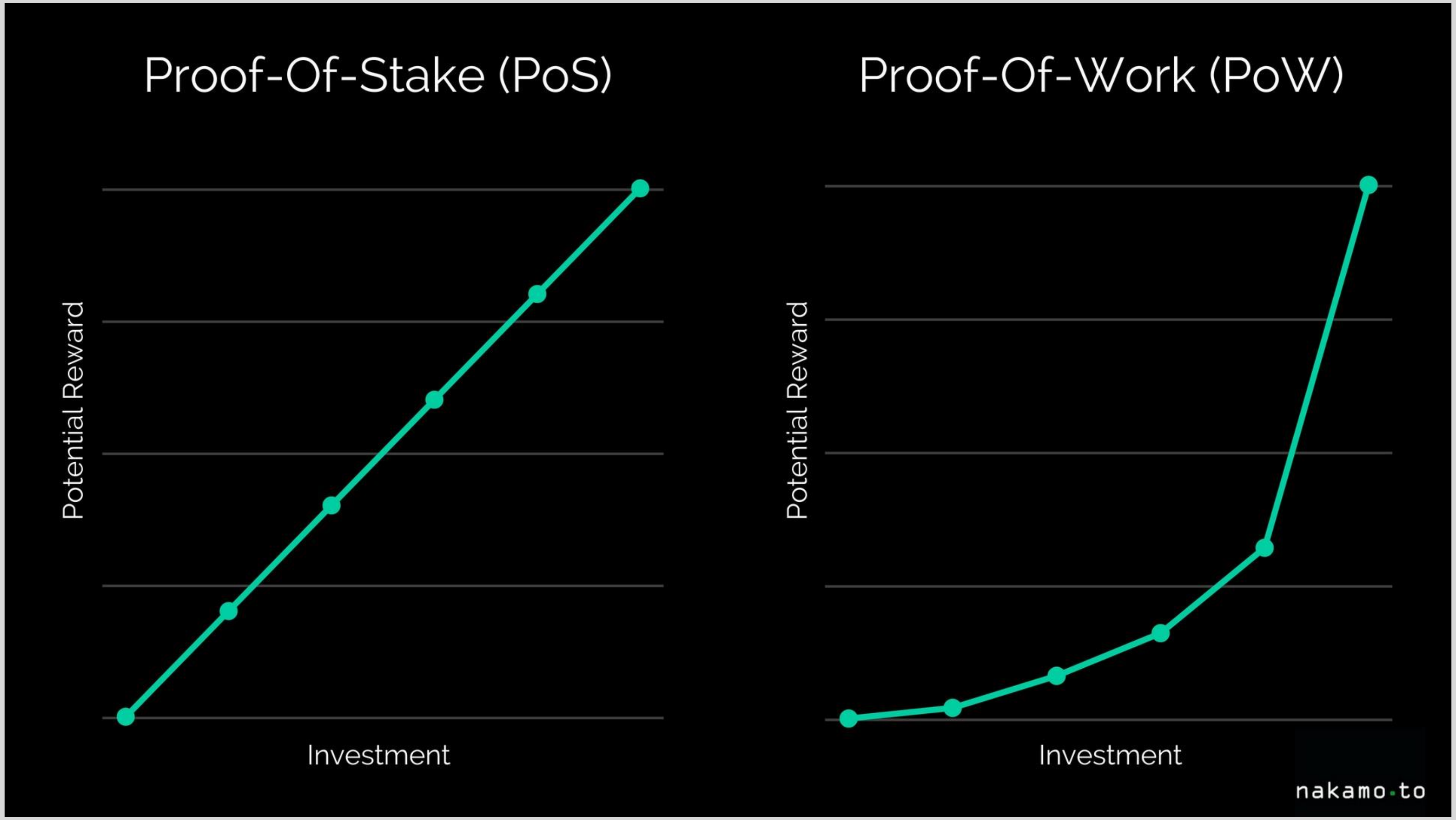
# PROOF-OF-STAKE



Stake (Security deposit)

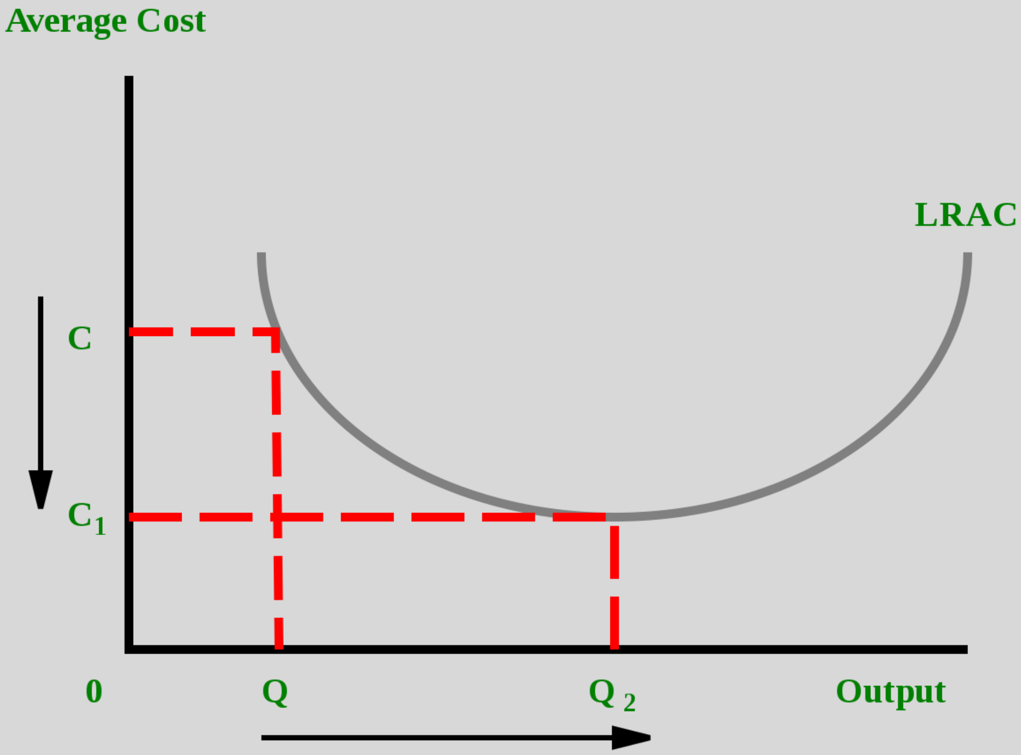
The size of stake determines the chances of a validator to be chosen to mint the next block

# PROOF-OF-STAKE



Wait, It's not seemed fair because PoS favors the rich, right?
Of course not!

# PROOF-OF-STAKE



With PoW, rich people can enjoy the power of **economies at scale**

1KWh = 3.000VNĐ but 1MWh != 3.000.000VNĐ
= 2.700.000VNĐ

# PROOF-OF-STAKE

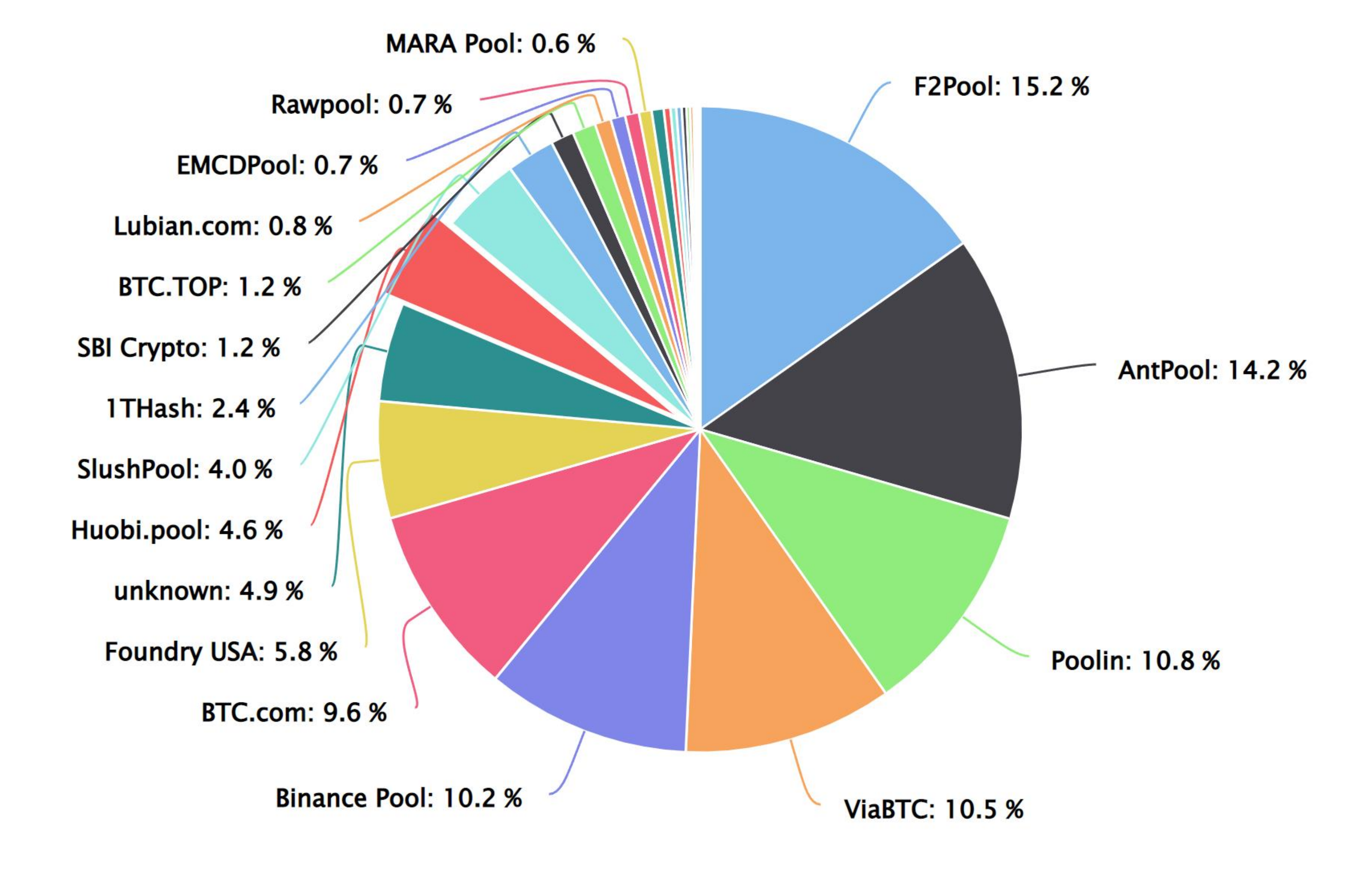
- If a node is chosen to validate the next block, she’ll check if all the transactions within it are indeed valid.
- If everything checks out, the node sign off the block and adds it into the blockchain.
- The reward for that block is the fees that are associated with each transaction.
- Validator will lose a part of their stake if they approve fraudulent transaction.
- We can trust the validator if the stake is higher than what them get from the transaction fees.
- If a node stops being a validator, her stake & all the fees she got will be hold for a certain period (The system still need to punish the validator if they discover some of blocks where fraudulent)

# PROOF-OF-WORK vs. PROOF-OF-STAKE

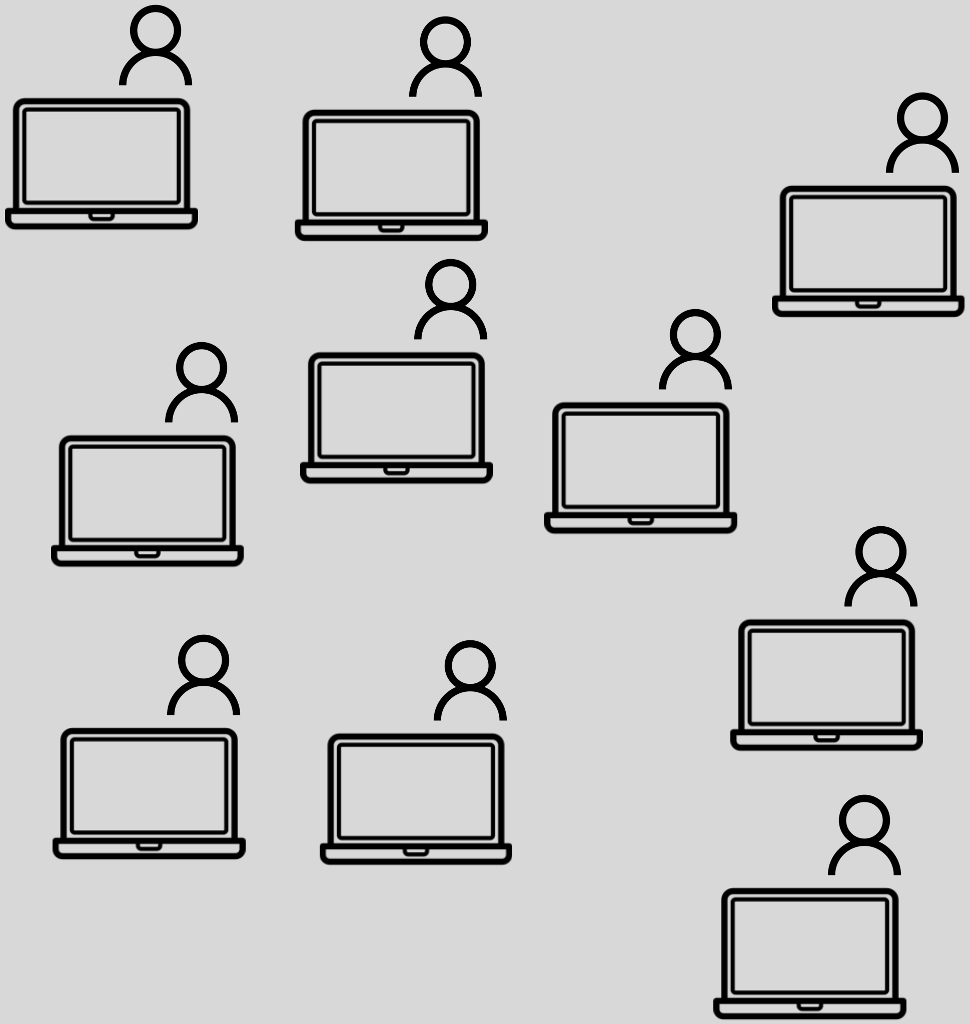
Everyone mines

Only a few selected Validators

# PROOF-OF-WORK vs. PROOF-OF-STAKE

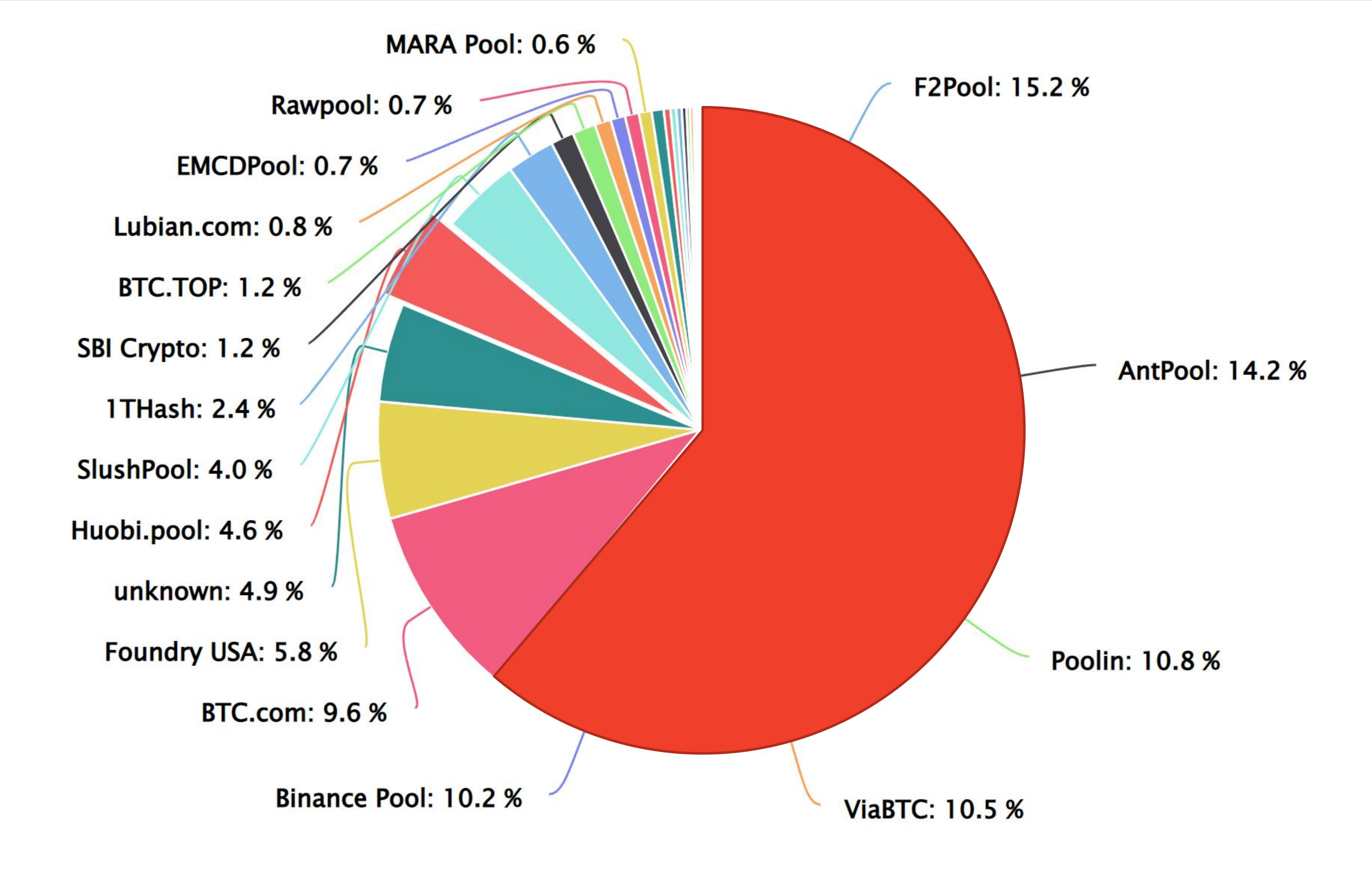


# PROOF-OF-WORK vs. PROOF-OF-STAKE



# PROOF-OF-WORK vs. PROOF-OF-STAKE

# PROOF-OF-WORK vs. PROOF-OF-STAKE



**51% Attack!**

# PROOF-OF-WORK vs. PROOF-OF-STAKE

Market capitalization of **SOLANA** (**SOL**) on November 22, 2021: **65.54 billion U.S. dollars**

**51% x market capitalization**

**= 33.4254 billion U.S. dollars**

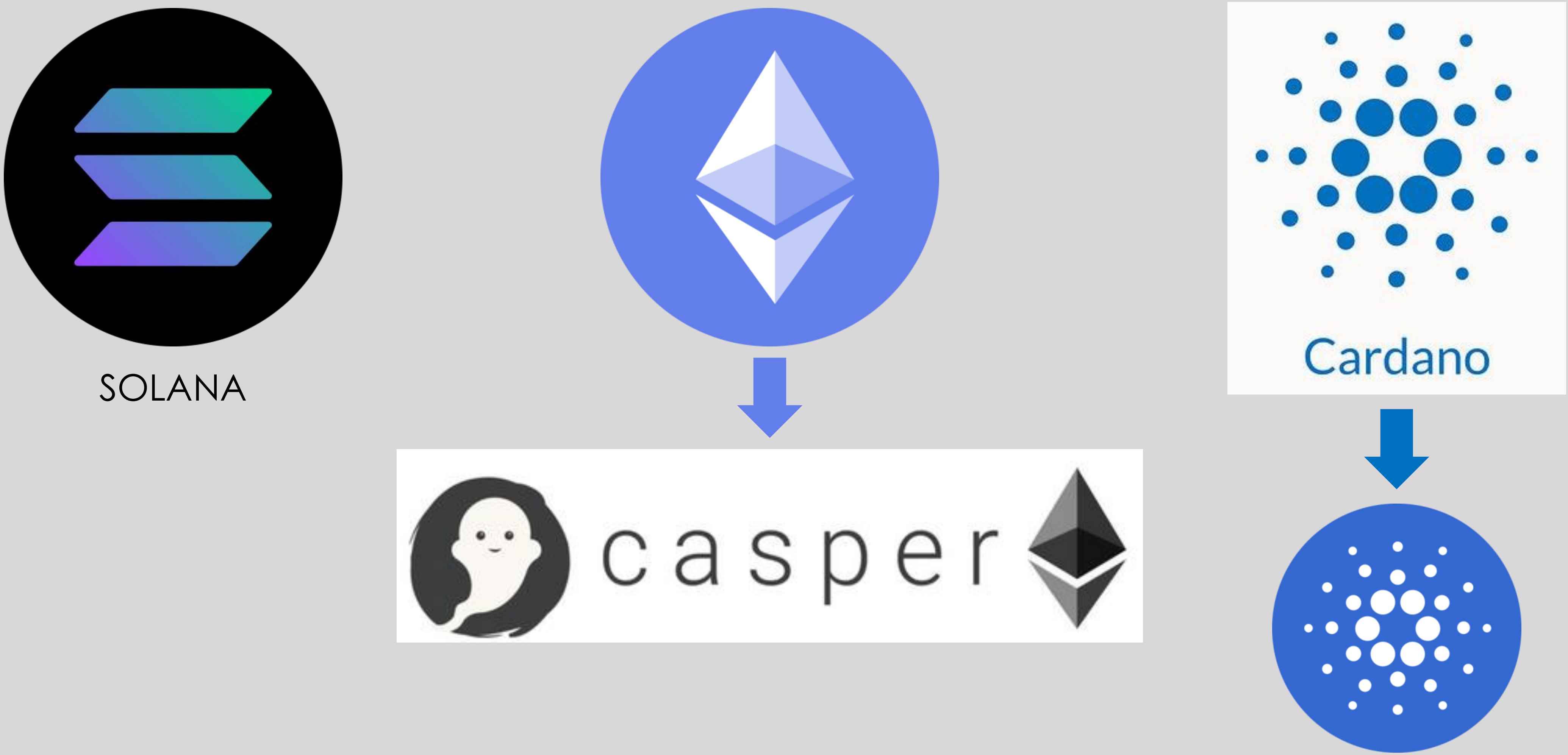
But the problem of PoS does not stop here …

# PROOF-OF-WORK vs. PROOF-OF-STAKE

- The algorithm must be careful how it select the validators. It's can't be completely random.
- The algorithm must have some mechanisms to choose the backup validator (as fallback) in case the chosen validator doesn't turn up her job.

- **Conclusion: PoS brings additional risk when compare with PoW.**

# PROOF-OF-STAKE APPLICATION



SOLANA

ADA