CSE446: Blockchain & Cryptocurrencies

Lecture – 12: Other Consensus Algorithms

BRAC UNIVERSITY

Inspiring Excellence

Agenda

- PoW Limitations
- Other consensus algorithms
    - Proof of Stake (PoS)
    - Delegated Proof of Stake (DPoS)
    - Byzantine Fault Tolerant PoS (BFT PoS)
        - Tendermint

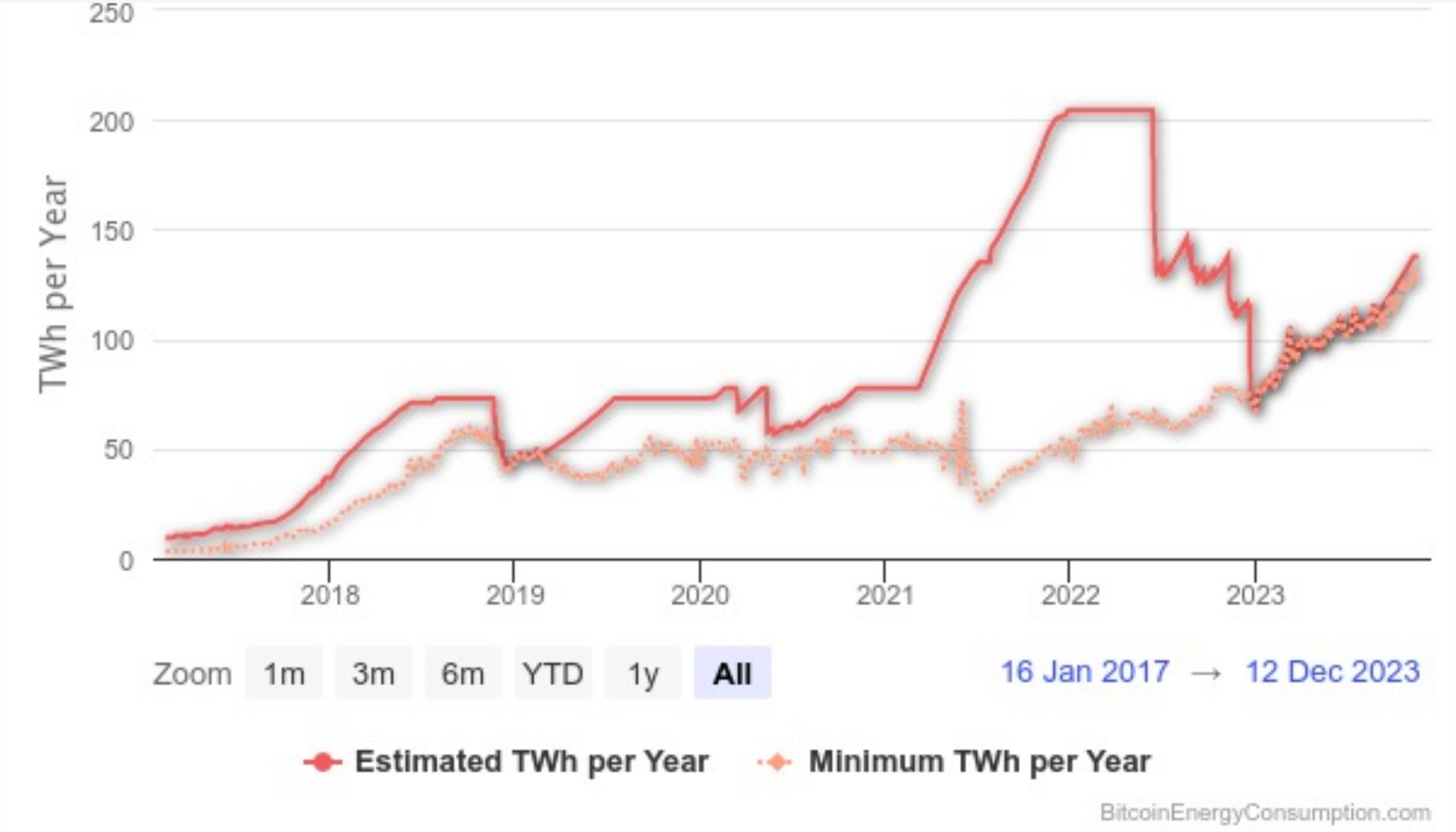
Pow Limitations

- There are a few major limitations of PoW
  - Energy consumption
  - Tragedy of commons
  - Absence of penalty
  - Delay in block finality (confirmation)

Pow Limitations: energy consumption

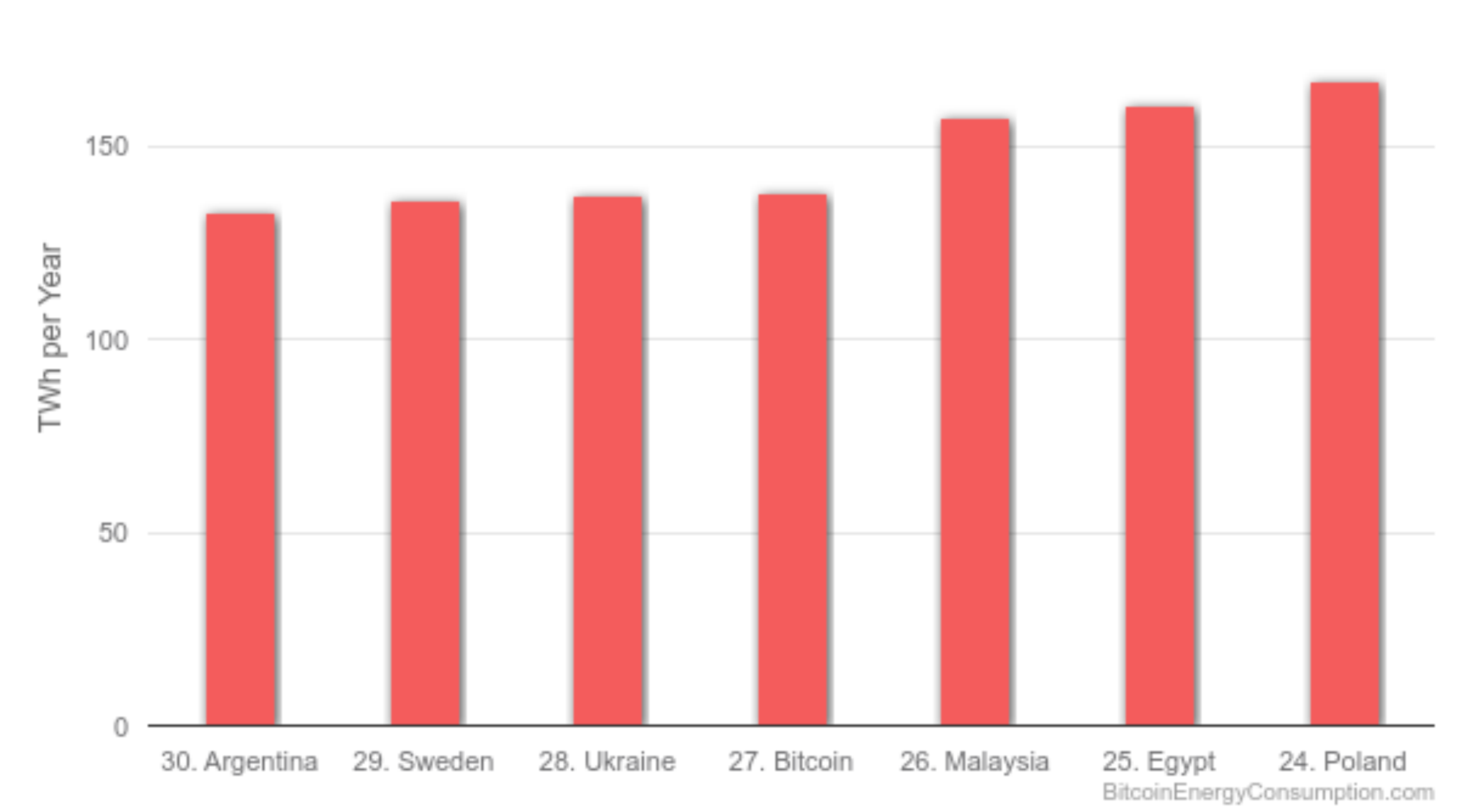
- Each PoW algorithm needs to consume electricity to compute the hash
- As the difficulty of the network starts to increase, so does the energy consumption
- The amount of consumed energy is quite significant when calculated over the whole network consisting of ASIC/GPU mining rigs all around the world

Pow Limitations: energy consumption



https://digiconomist.net/bitcoin-energy-consumption

Pow Limitations: energy consumption by country



https://digiconomist.net/bitcoin-energy-consumption

Pow Limitations: tragedy of commons

- This situation occurs in a crypto-currency if it is deflationary in nature with limited supply, e.g. Bitcoin
- It has been argued when the reward of creating a new block in Bitcoin will reach nearly zero
    - the miners will have to solely rely on the transaction fees to cover their expenses
- This might create an unhealthy competition among the miners to include as many transactions as possible, just to maximise one’s profit

Pow Limitations: tragedy of commons

- The consequence of this is that transaction fees will keep decreasing
- This might lead to a situation that miners cannot make enough profit to continue the mining process
- Eventually, more and more miners will leave the mining process
    - This might lead toward 51% attacks or other scenarios that might de-stabilise the Bitcoin network

Pow Limitations: absence of penalty

- PoW algorithms are altruistic in nature in the sense that they reward behaving miners
  - However, they do not penalise a misbehaving miner
- One example is that a miner can collude with a group of miners (a phenomenon known as selfish mining) to increase its profitability in an illegitimate way

Pow Limitations: absence of penalty

- In addition, a miner can engage in Denial-of-Service attacks by just not forwarding any transaction or block within the network
- Furthermore, such malicious miners can join forces to engage in the spawn-camping attack
  - Launching DoS attacks simultaneously over and over again to render the blockchain network useless
- A penalty mechanism would disincentivise any miner to engage in any type of malicious misbehave

Pow Limitations: delay in finality

- Finality is the assurance or guarantee that crypto-currency transactions cannot be altered, reversed, or cancelled after they are completed
- Finality is used to measure the amount of time one has to wait for a reasonable guarantee for a transaction to be confirmed (included in a block)
- In blockchain technology, transactions are termed immutable due to its finality nature
- The latency level of a blockchain will ultimately affect the chain's finality rate

https://academy.binance.com/en/glossary/finality

Pow Limitations: delay in finality

- Finality is an essential feature for ventures accepting cryptocurrencies because
  - waiting endlessly on a blockchain network can have a high adverse effect for businesses or enterprises that accept crypto as a means of payment
- When creating a payment system, to be effective, it is crucial to have low latency
- If you were to have to wait for 10 minutes every time you wished to purchase anything, it would quickly become very inconvenient to go shopping
- However, most blockchain protocols only show a probabilistic transaction finality
  - meaning that transactions are not automatically or instantly final but become "more and more final" over time (as more blocks are confirmed)
  - For Bitcoin, it is estimated that one has to wait 6 blocks, around 1 hour, before we can say that a transaction is final with a reasonable guarantee

https://academy.binance.com/en/glossary/finality

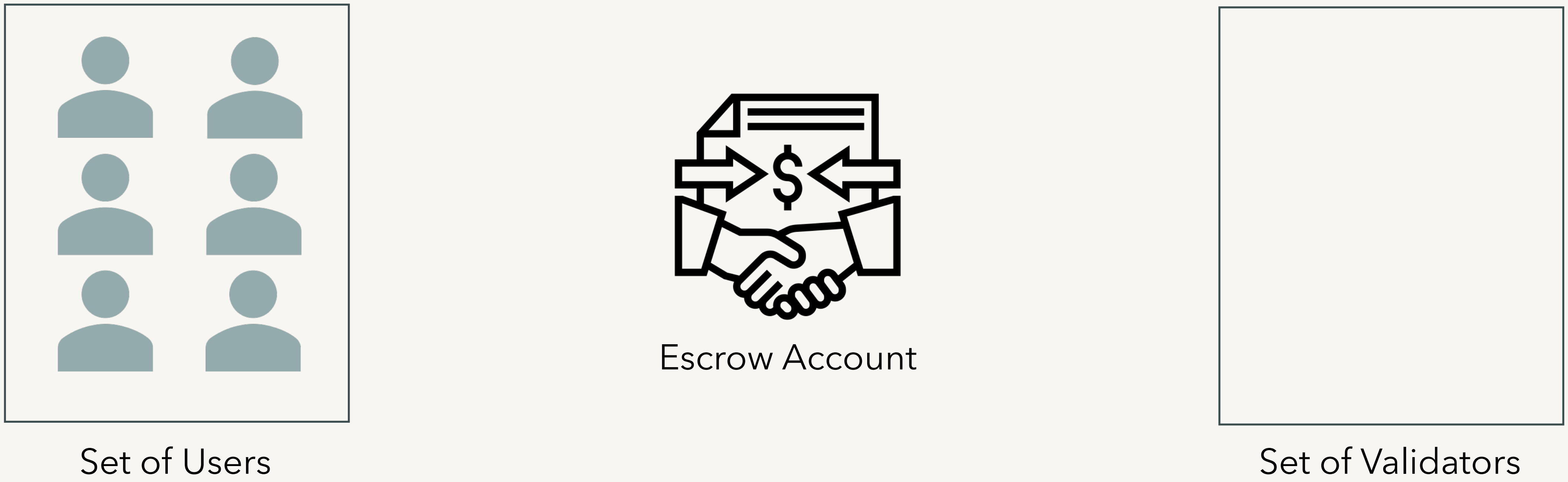
Proof of Stake (PoS)

- In PoS, the nodes who would like to participate in the block creation process must prove that they own a certain number of coins at first
- Besides, they must lock a certain amount of its currencies, called stake, into an escrow account in order to participate in the block creation process
- The stake acts as a guarantee that it will behave as per the protocol rules
- The node escrows its stake in this manner is known as the stakeholder, staker, validator, leader, forger, or minter in PoS terminology
- The minter can lose the stake, in case it misbehaves

Proof of Stake

- In essence, when a stakeholder escrows its stake, it implicitly becomes a member of an exclusive group
- Only a member of this exclusive group can participate in the block creation process
- How much block a minter can generate depends on their size of stakes
- The stakeholder who produce blocks are rewarded in one of the two different ways
  - Either it can collect the transaction fees within the block, or
  - It is provided a certain amount of currencies that act as a type of interest against their stake

Proof of Stake

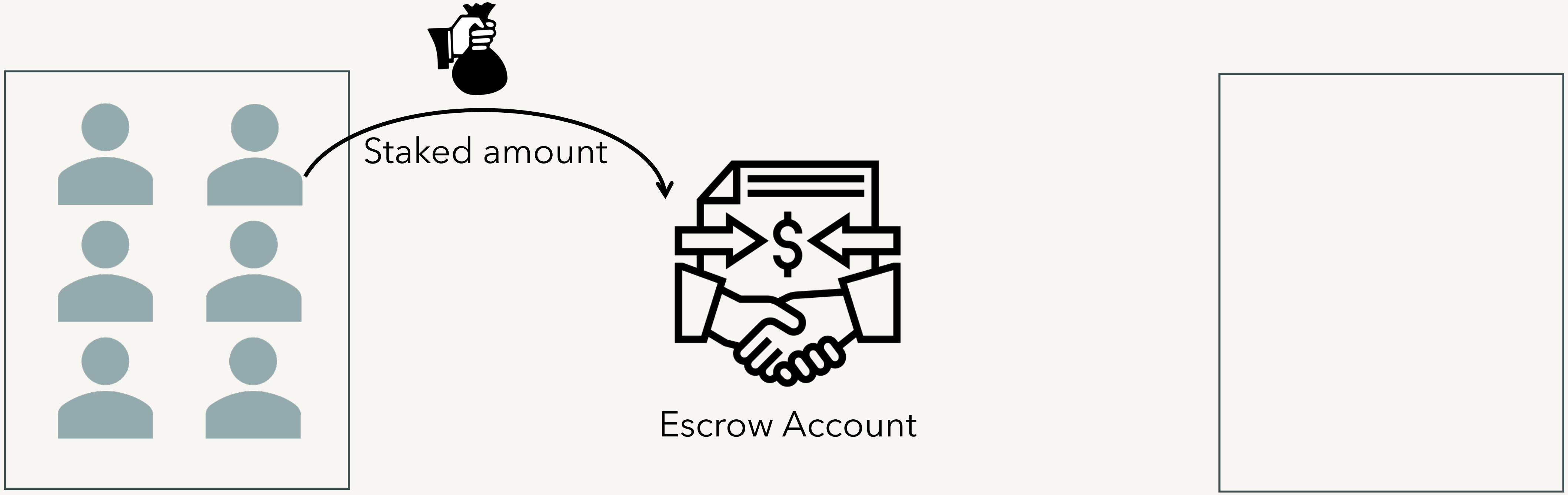


Set of Users

Escrow Account

Set of Validators

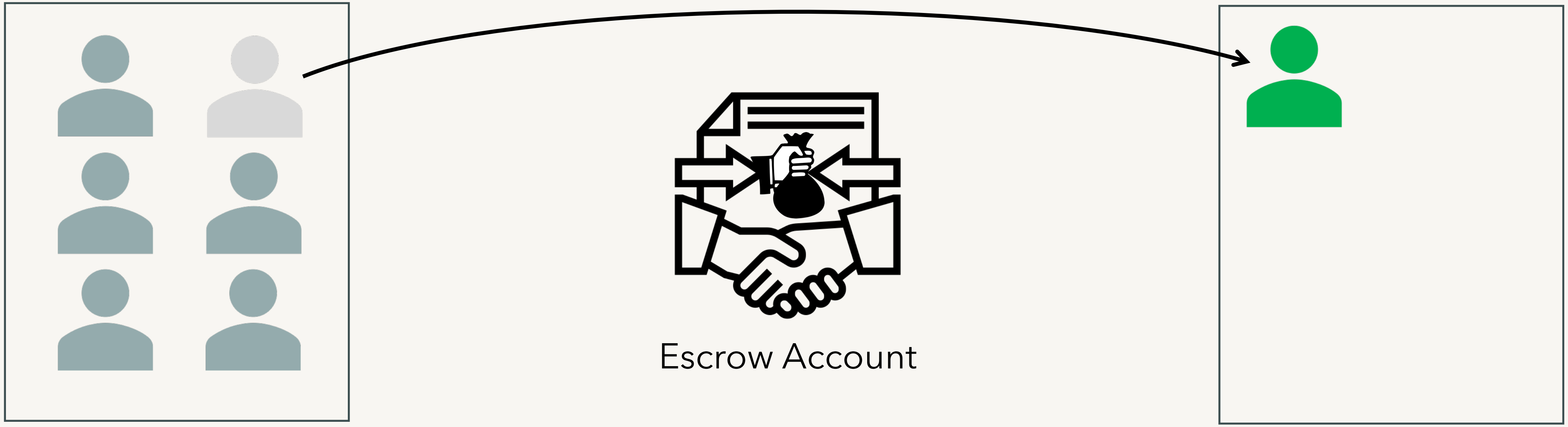
Proof of Stake



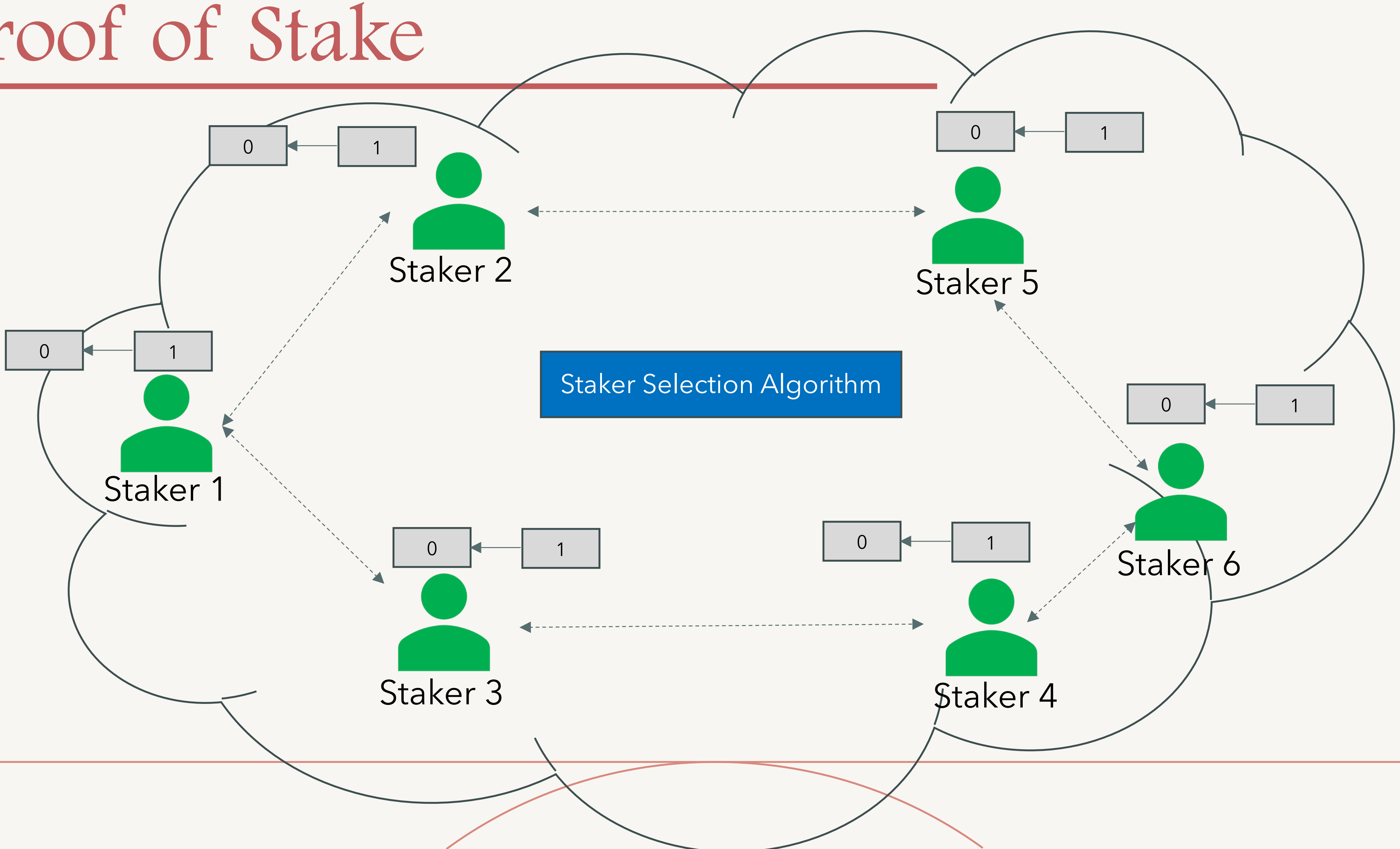
Set of Users

Set of Validators

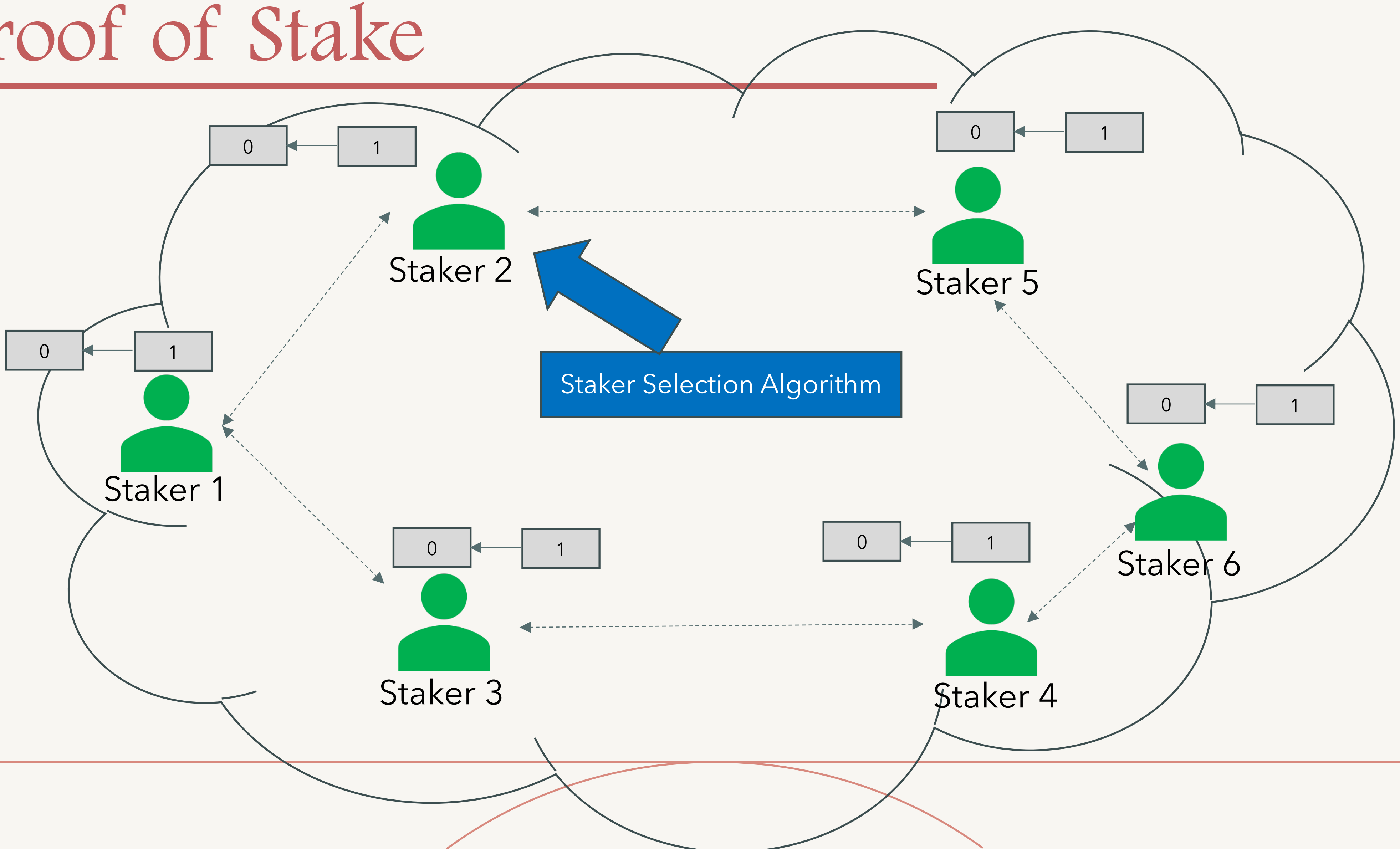
Proof of Stake



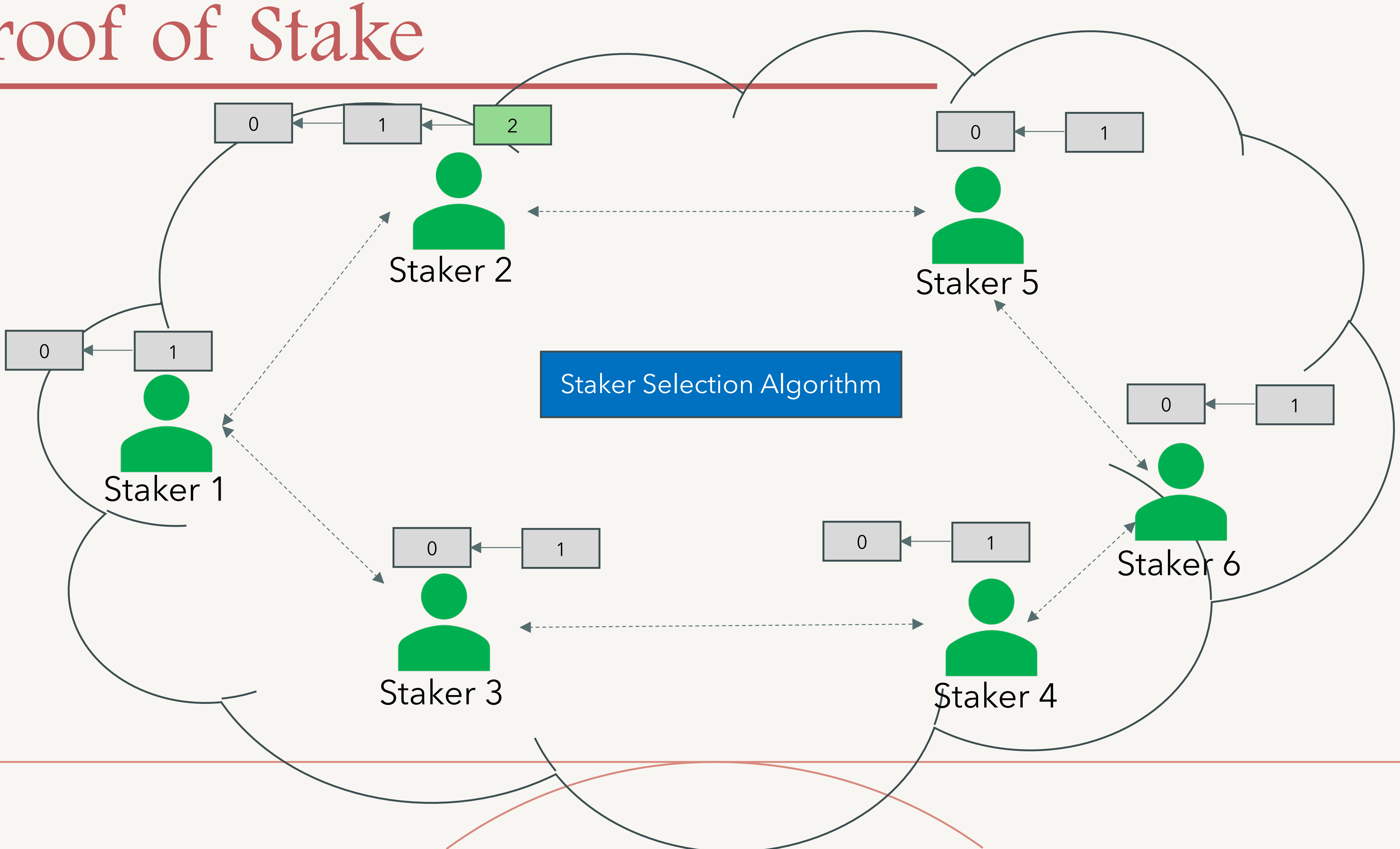
Proof of Stake



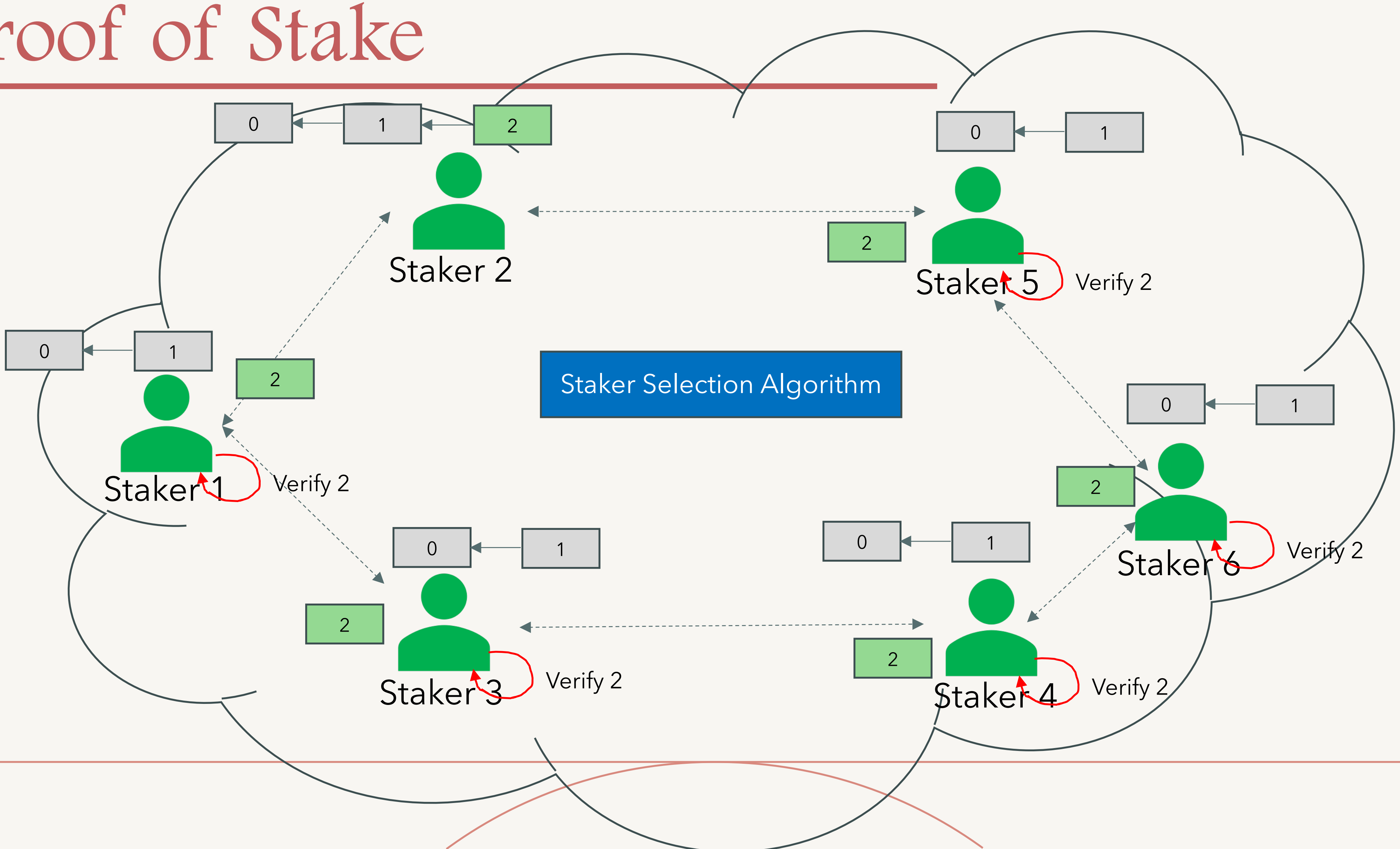
Proof of Stake



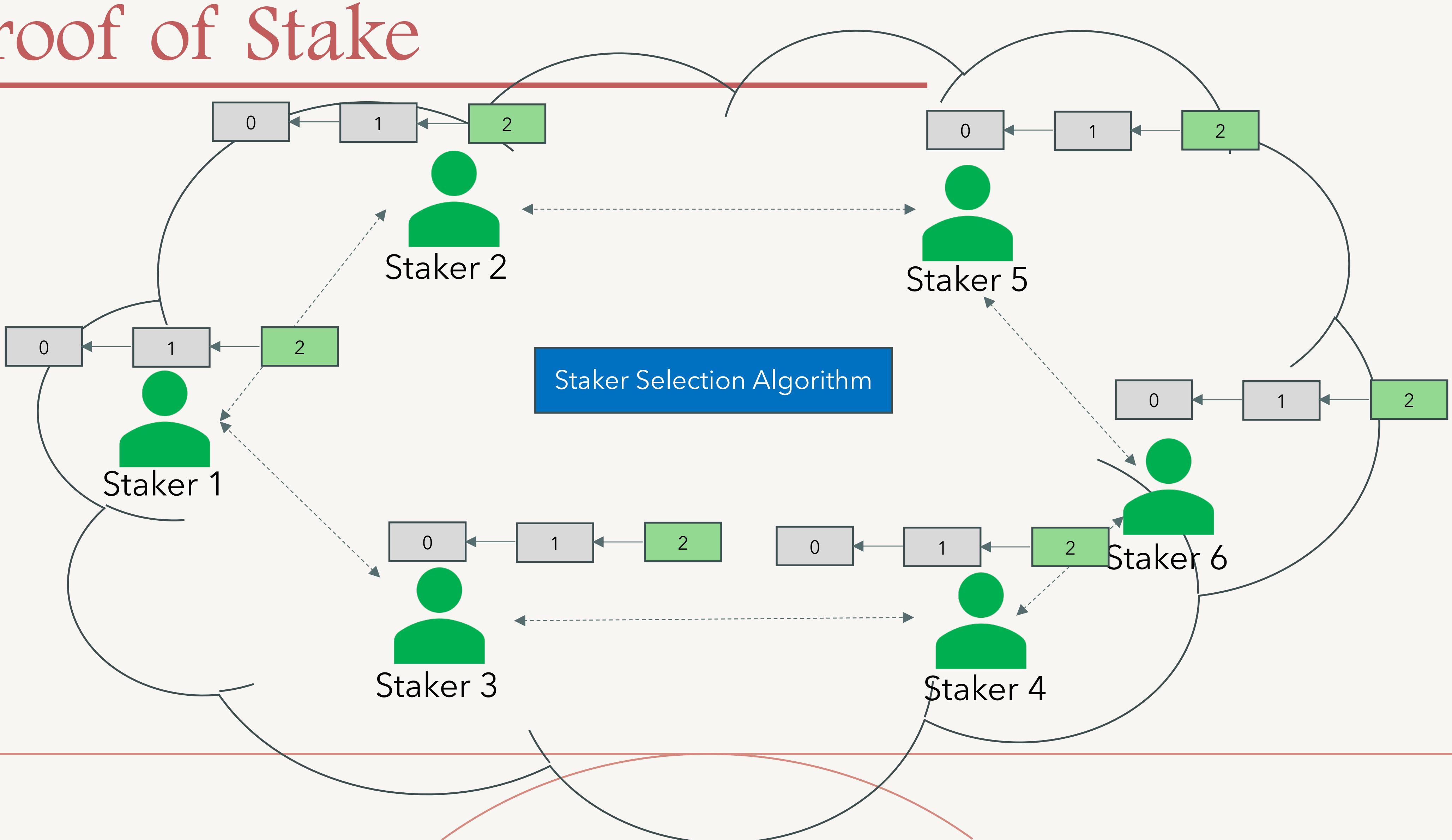
Proof of Stake



Proof of Stake



Proof of Stake



PoS: Bootstrapping issue

- One of the major barriers in a PoS algorithm is how to generate the initial coins
- A fair distribution of coins among the stakeholders are essential to ensure a secure PoS algorithm
- This is known as the bootstrapping problem
- There are two ways to solve the bootstrap issue:
  - Pre-mining
  - PoW to PoS transition

PoS: Bootstrapping issue

- Pre-mining:
  - A set of coins are pre-mined, which are then sold before the launch of the system in an IPO (Initial Public Offering) or ICO (Initial Coin Offering)
- PoW-PoS transition
  - The system starts with a PoW system to fairly distribute the coins among the stakeholders
  - Then, it slowly transitions towards the PoS system
  - Ethereum took this approach

DPoS

- Delegated Proof of Stake (or DPoS in short) is a form of consensus algorithm in which reputation scores or other mechanisms are used to select the set of (delegated) validators
- Even though it has the name Proof of Stake associated with it, it is quite different from other PoS algorithms
- In DPoS, users of the network vote to select a group of delegates (or witnesses) who are responsible for creating blocks
- Delegates are the only entities who can propose new blocks

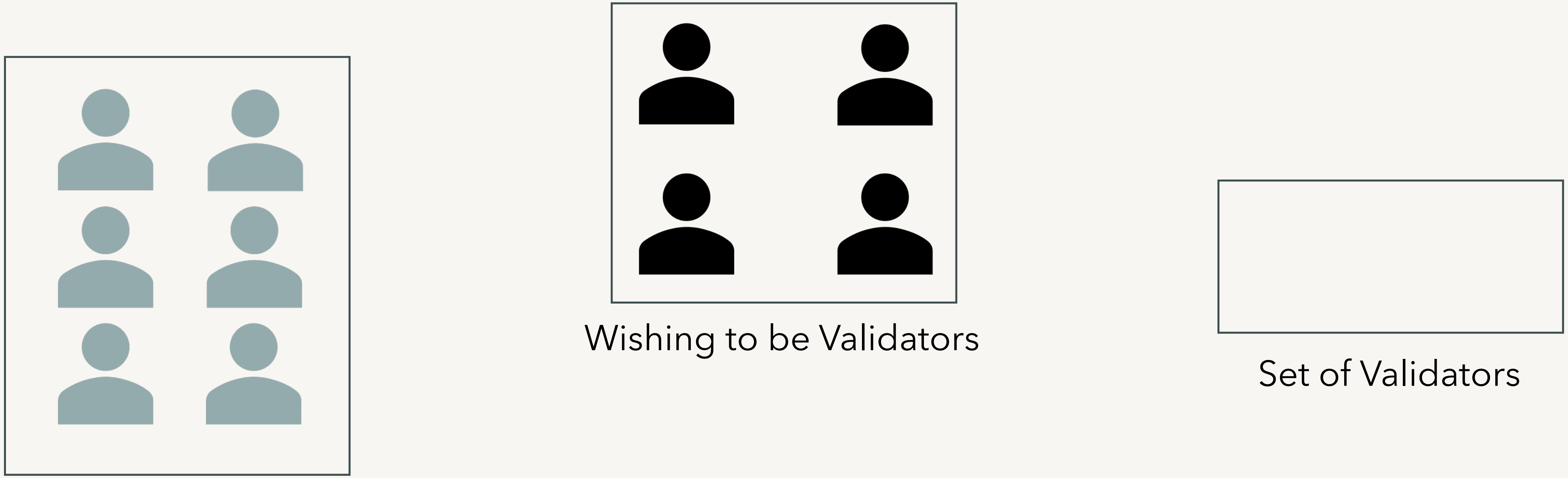
DPoS

- For each round, a leader is selected from the set of delegates who can propose a block
- How such a leader is chosen depends on the respective blockchain system
- The leader gets rewards for creating a new block, and is penalised and de-listed from the set of validators if it misbehaves

DPoS

- The delegates themselves compete with each other to get included in the validator list
- In such, each validator might offer different levels of incentives for the voters who vote for it
- For example, if a delegate is selected to propose a block, it might distribute a certain fraction of its reward among the users who have voted for the delegate
- Since the number of validators is small, the consensus finality (confirmation) can be fast

DPoS

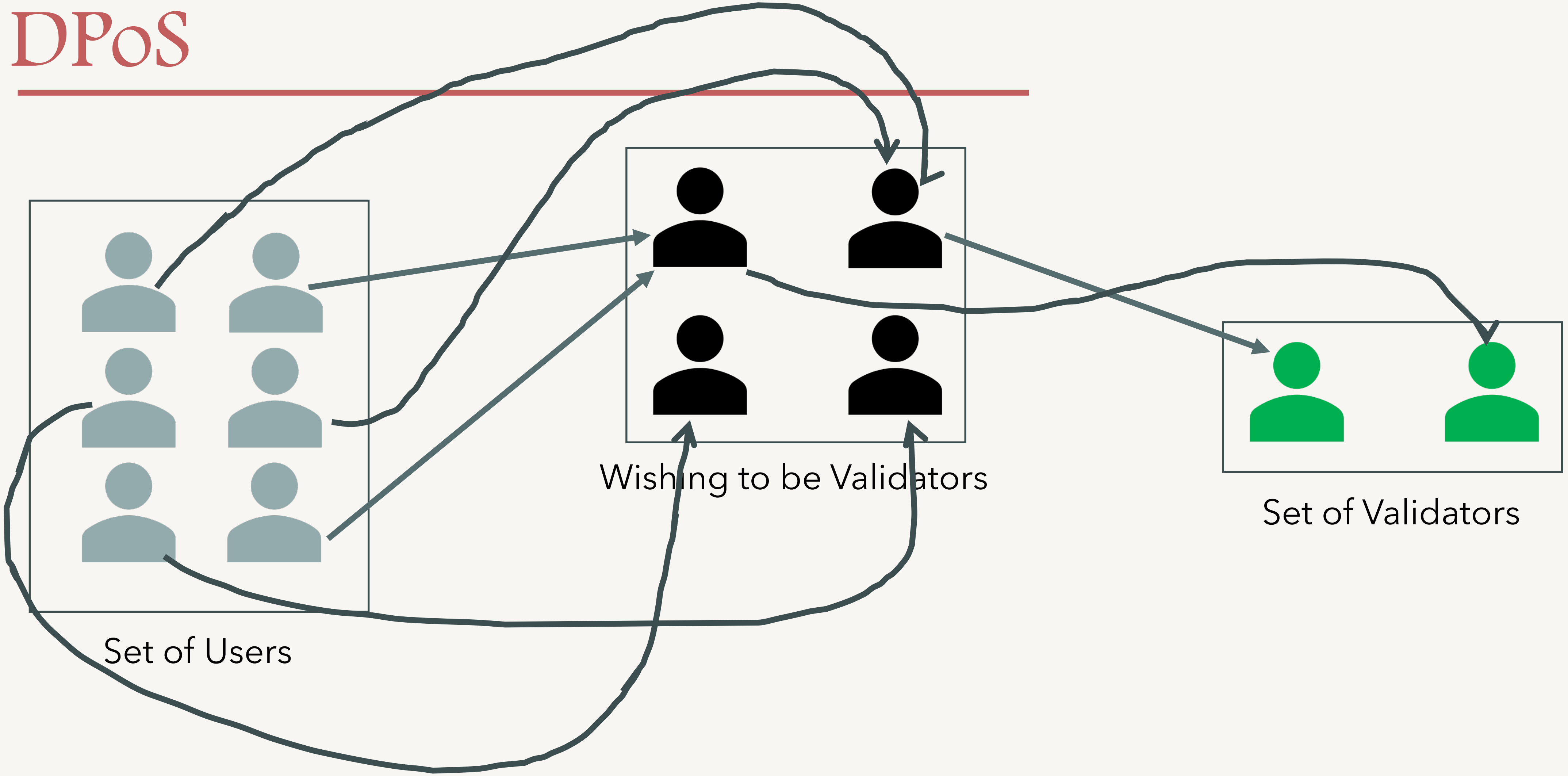


Wishing to be Validators

Set of Validators

Set of Users

DPoS



DPoS: EOS

- EOS is the first and the most widely known DPoS crypto-currency and smart-contract platform
- The DPoS consensus algorithm of EOS utilises 21 validators, also known as Block Producers (BPs)
- These 21 validators are selected with votes from EOS token (currency) holders
- The number of times a particular BP is selected to produce a block is proportional to the total votes received from the token holders

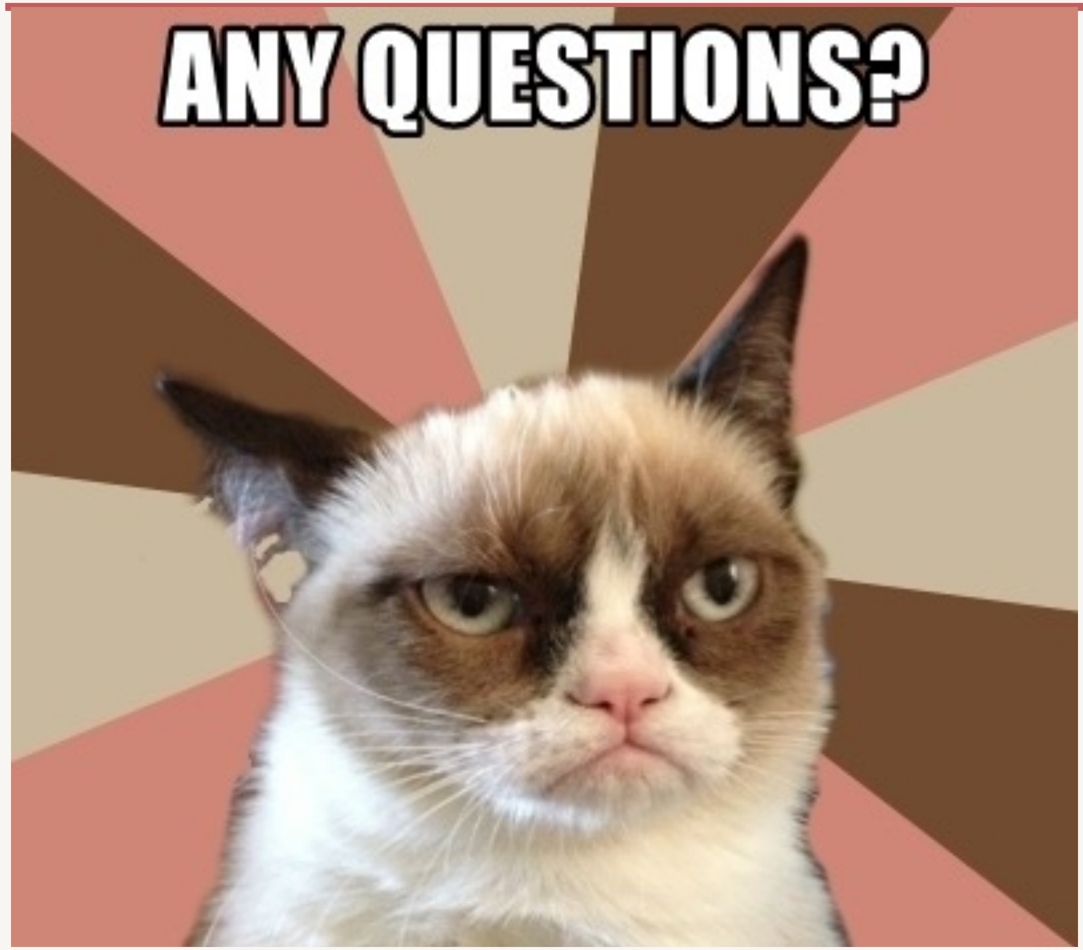
DPoS: EOS

- Blocks in EOS are produced in rounds where each round consists of 21 blocks
- At the beginning of each round, 21 BPs are selected
- Next, each of them gets a chance to create a block in pseudo-random fashion within that particular round
- Once a BP produces a block, other BPs must validate the block and reach into a consensus
- A block is confirmed only when the (+2/3) majority of the BPs reach the consensus regarding the validity of the block
- Once this happens, the block and the associated transactions are regarded as confirmed or final, so no fork can happen

Finality: Bitcoin vs EOS

Blockchain	Consensus	Avg. time per block	Avg. time to finality
Bitcoin	PoW	10 minutes	60 minutes (6 confirmations)
EOS	DPoS	0.5 - 1 second	2-3 seconds (2-3 commitments)

https://academy.binance.com/en/glossary/finality


ANY QUESTIONS?