Practical Blockchain

Module 4: Consensus Algorithms

Scope

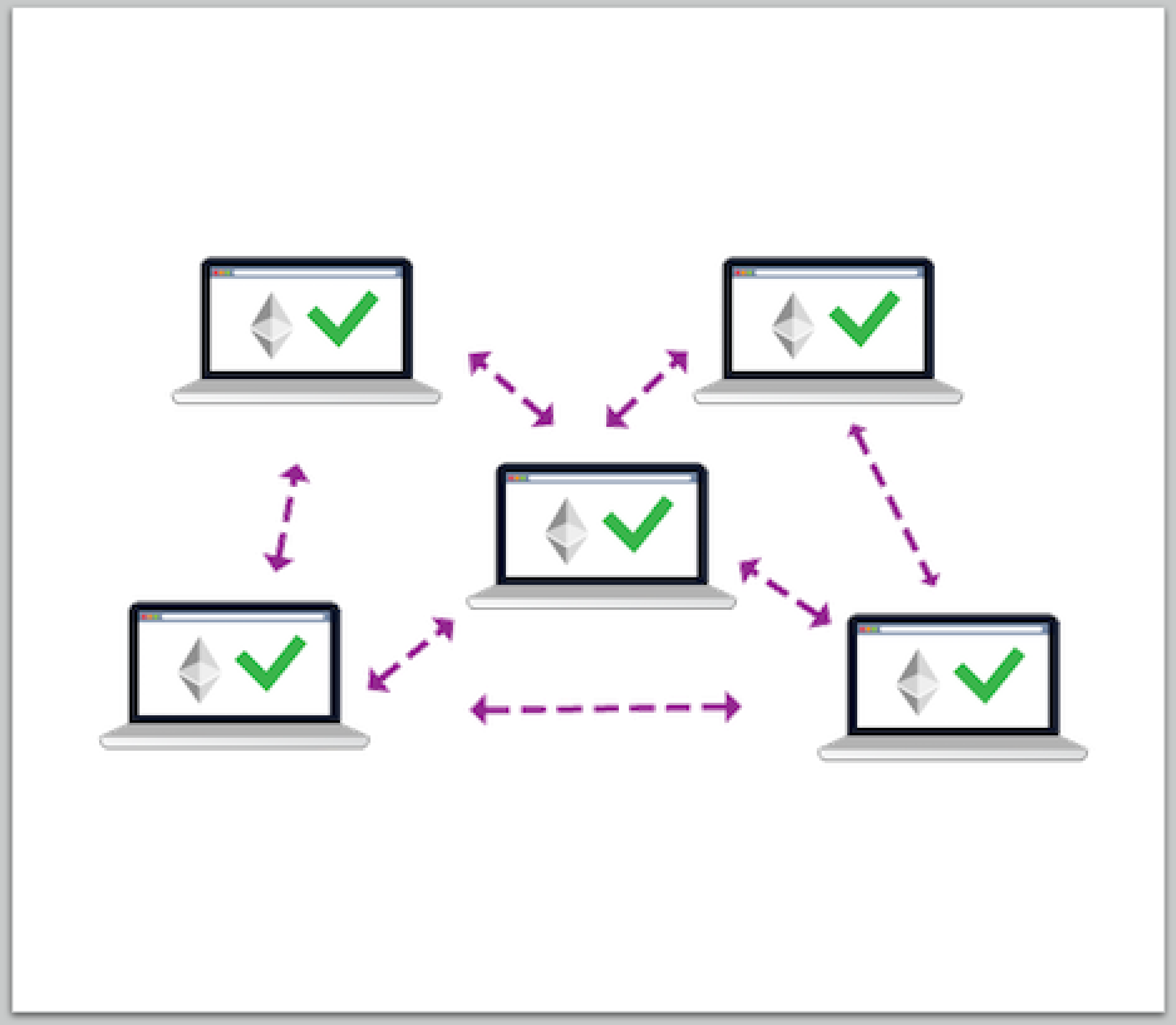
- Overview
- Byzantine Fault
- Common Consensus Protocols
- Hands-on: Setting up a blockchain with a different consensus mechanism

Overview

One of blockchain's most important features is the consistency and security it provides to stored data.

In blockchain, consistency refers to an agreement among the various network nodes as to the state of the stored data.

A consensus mechanism refers to an algorithm that assist nodes to reach such an agreement on the status of a network.

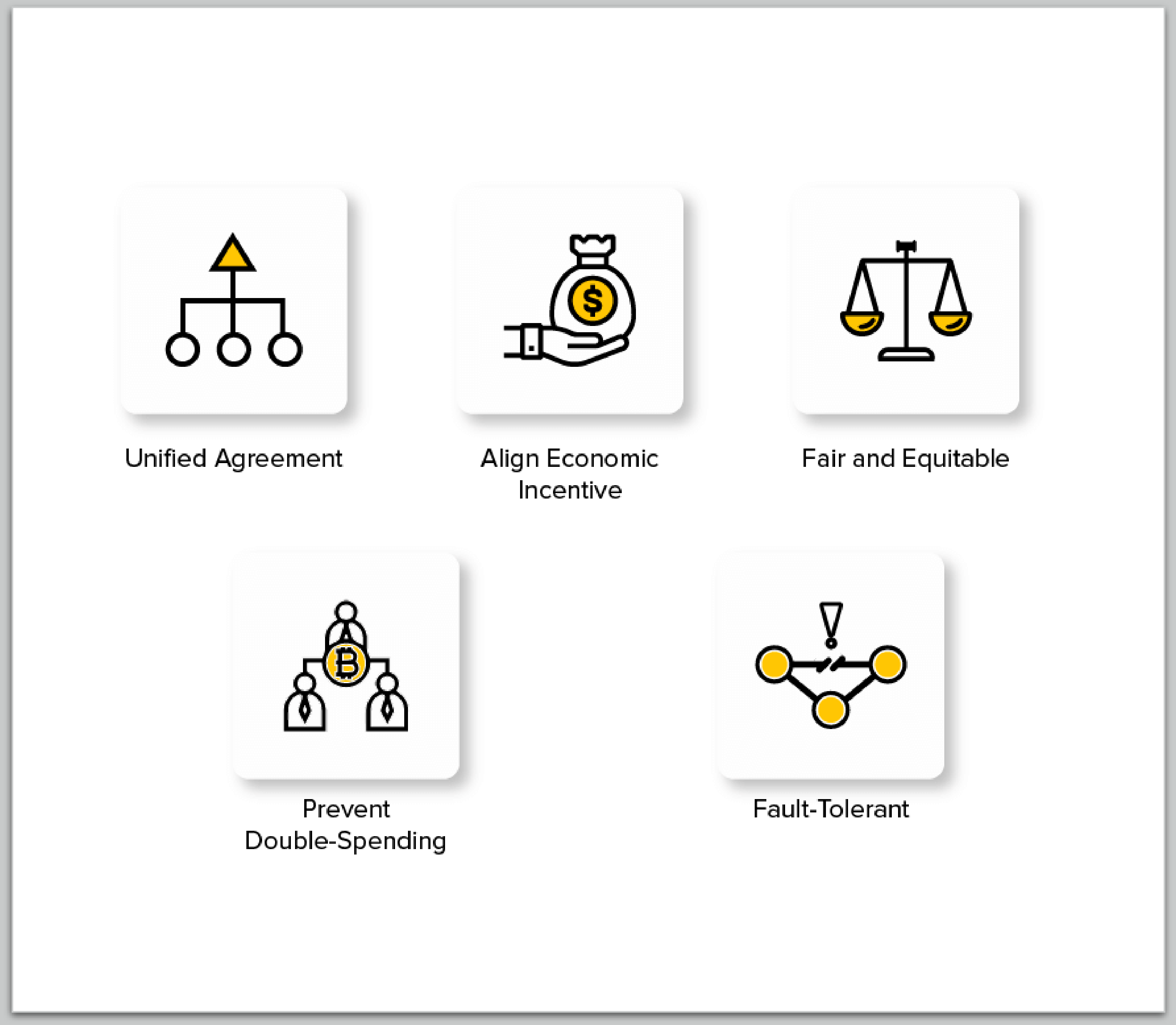


Objectives

Unified agreement: The primary goal of any consensus mechanism is to solve the core problem that underlies distributed ledger systems, that is, to reach a unified agreement regarding the state of the network.

Prevent double-spending: Chapter 2 introduced double-spending as one of the main problems faced by digital currencies.

Self-regulation: The consensus mechanism supports the self-regulating aspects of a trustless system, which requires aligning the interests of all network participants.



Unified Agreement

Align Economic Incentive

Fair and Equitable

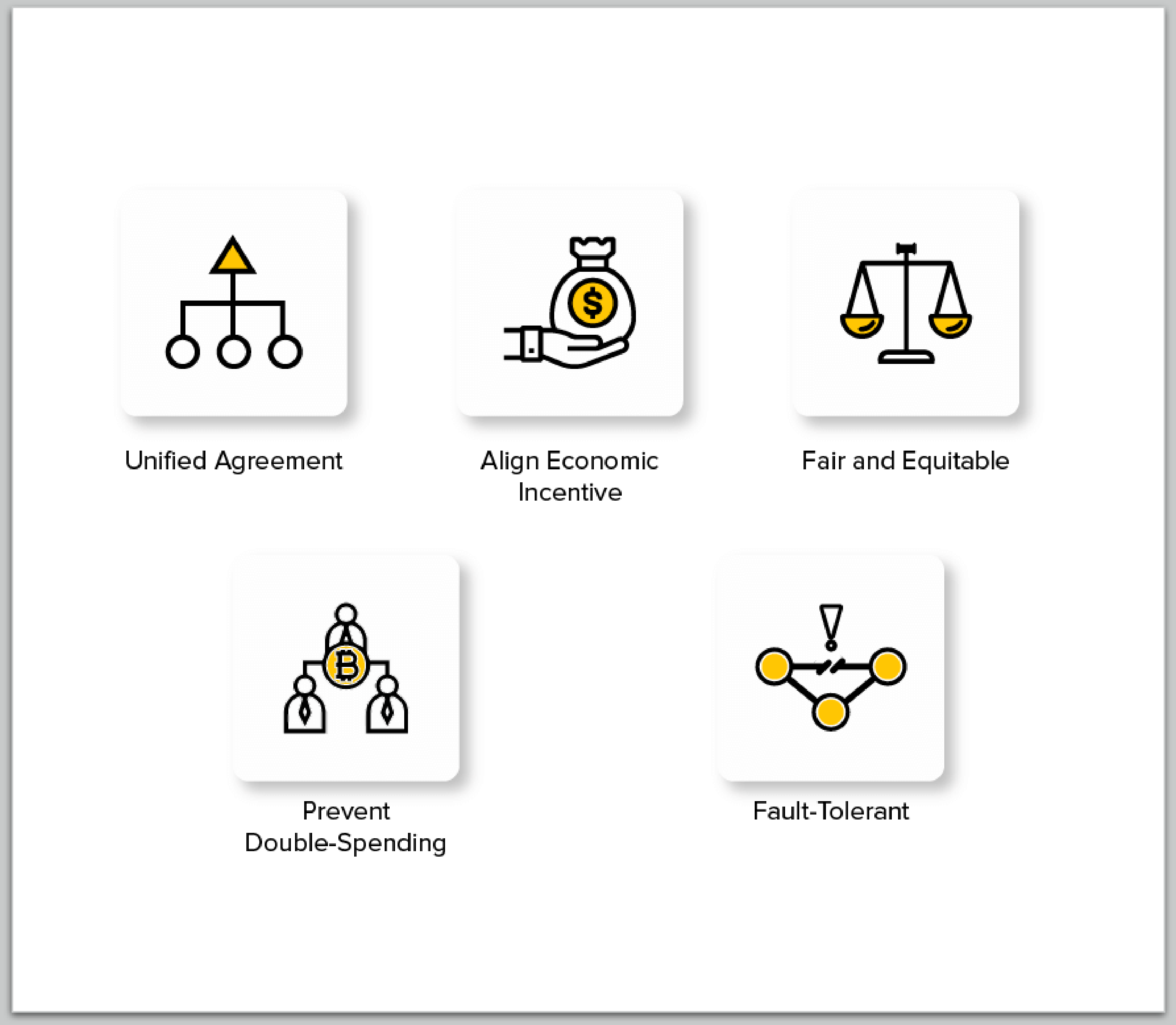
Prevent Double-Spending

Fault-Tolerant

Objectives

Fair participation: Blockchain is a peer-to-peer network with a low barrier to setting up new nodes and becoming a participant.

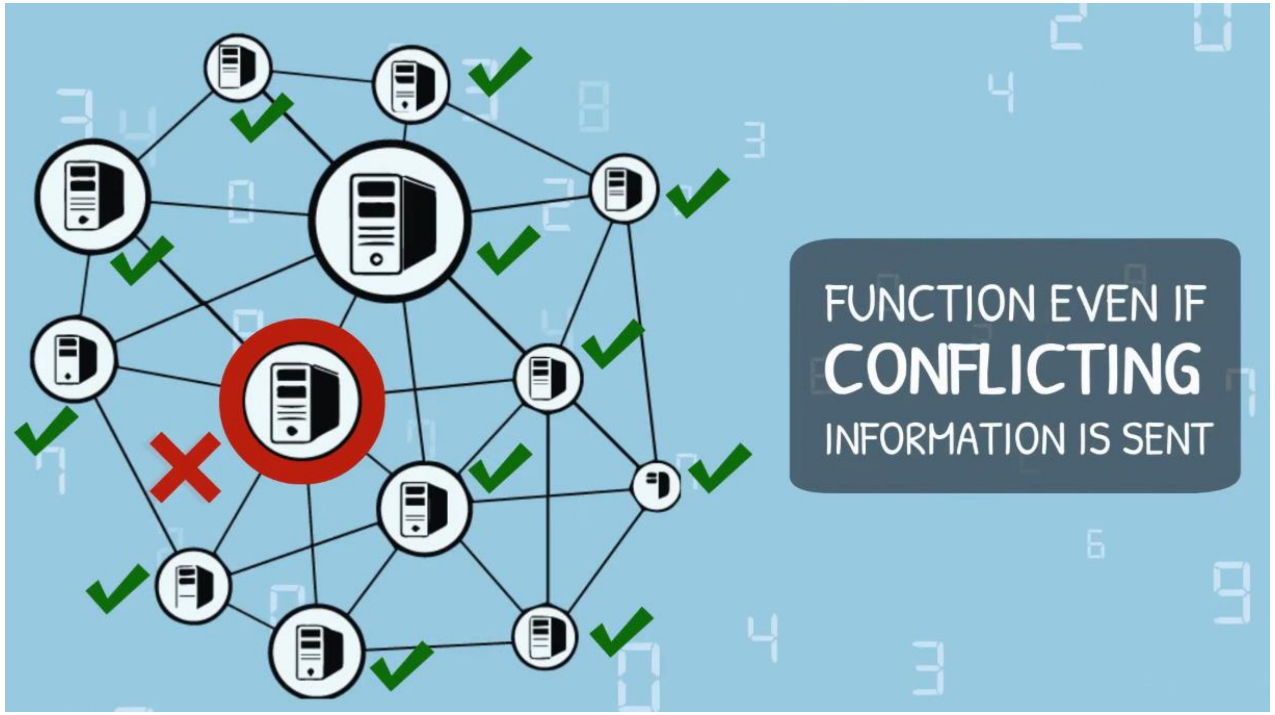
Provide fault-tolerance: In the computing space, fault tolerance describes a computer system whose design provides immediate and uninterrupted replacement



Byzantine Fault Tolerance

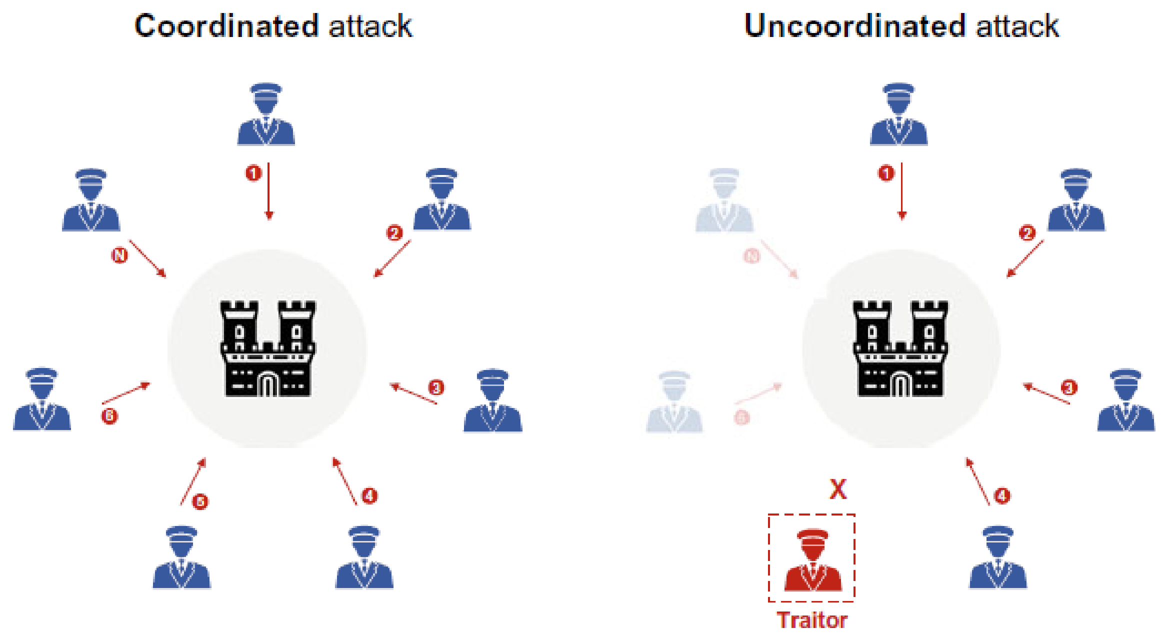
Byzantine fault describes the condition of a distributed computer system in which components can fail, and information regarding component failure is not guaranteed.

Byzantine fault tolerance (BFT) is the property of a system that is able to continue operating even if some of the nodes fail or act maliciously.



Byzantine Generals' Problem

"Byzantine generals' problem," is a scenario wherein actors must agree on a concerted strategy to avoid catastrophic failure, but some of the actors are inherently unreliable



Byzantine Generals' Problem

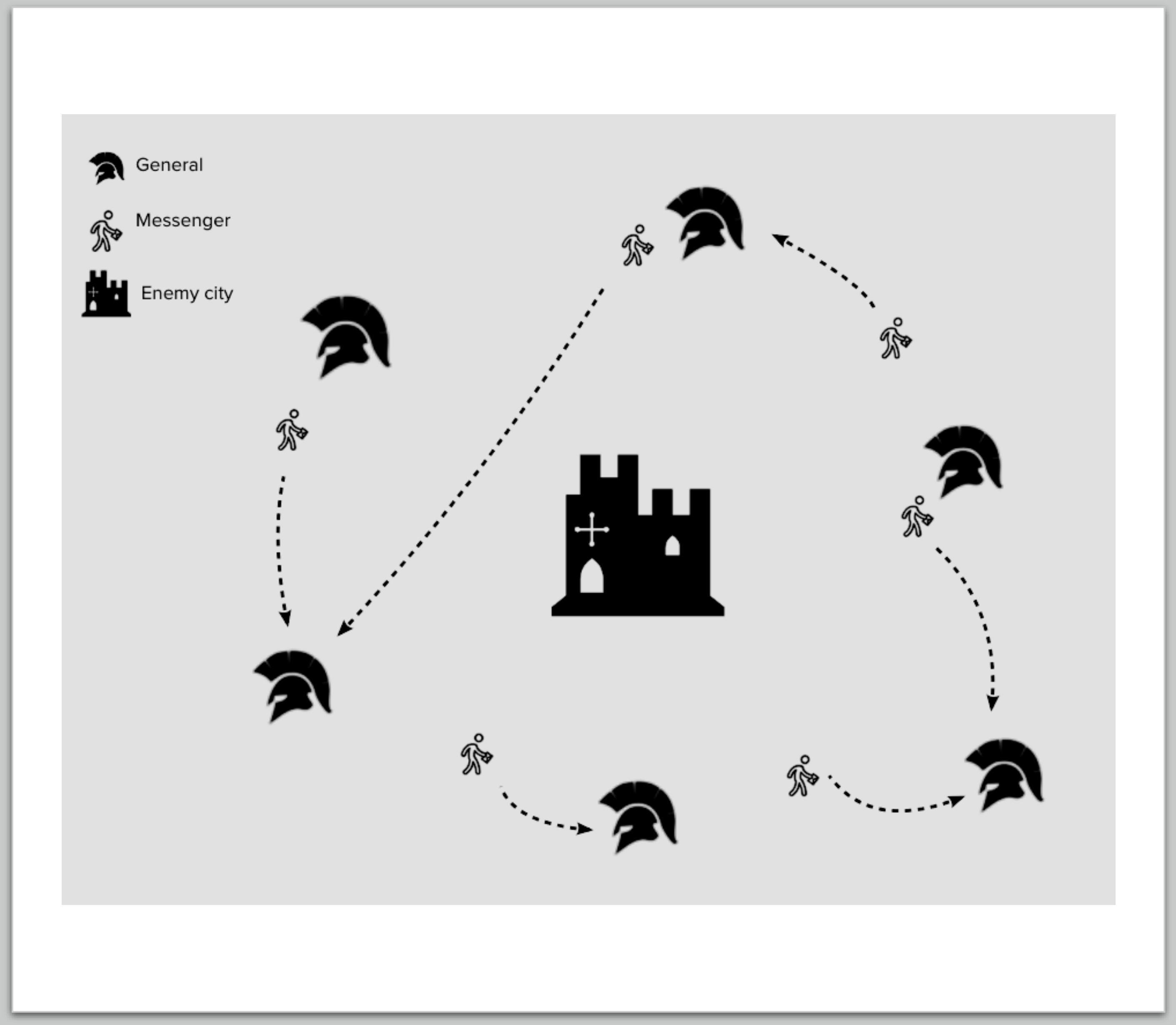
One general sends a message to other Generals: Lets attack at 11:00 today

Failure scenarios

One of the generals can be a traitor and purposely pass a wrong message to mislead other generals

The message can be lost on the way

The message can arrive late



Byzantine Generals’ Problem

In computer science Byzantine Generals’ Problem is used as a thought experiment to explore the underlying challenge of how to reach consensus among parties in an imperfect environment where there are failures, fraud etc

This dilemma can be applied to the context of blockchains with each general representing a network node.

The majority of nodes have to agree and execute the same action in order to avoid complete failure.

Consensus algorithm is the mechanism through which a blockchain network reach consensus

Common Consensus Protocols

Proof of Work

Proof of Stake

Proof of Capacity/Space

Delegated Proof of Stake

Proof of Authority

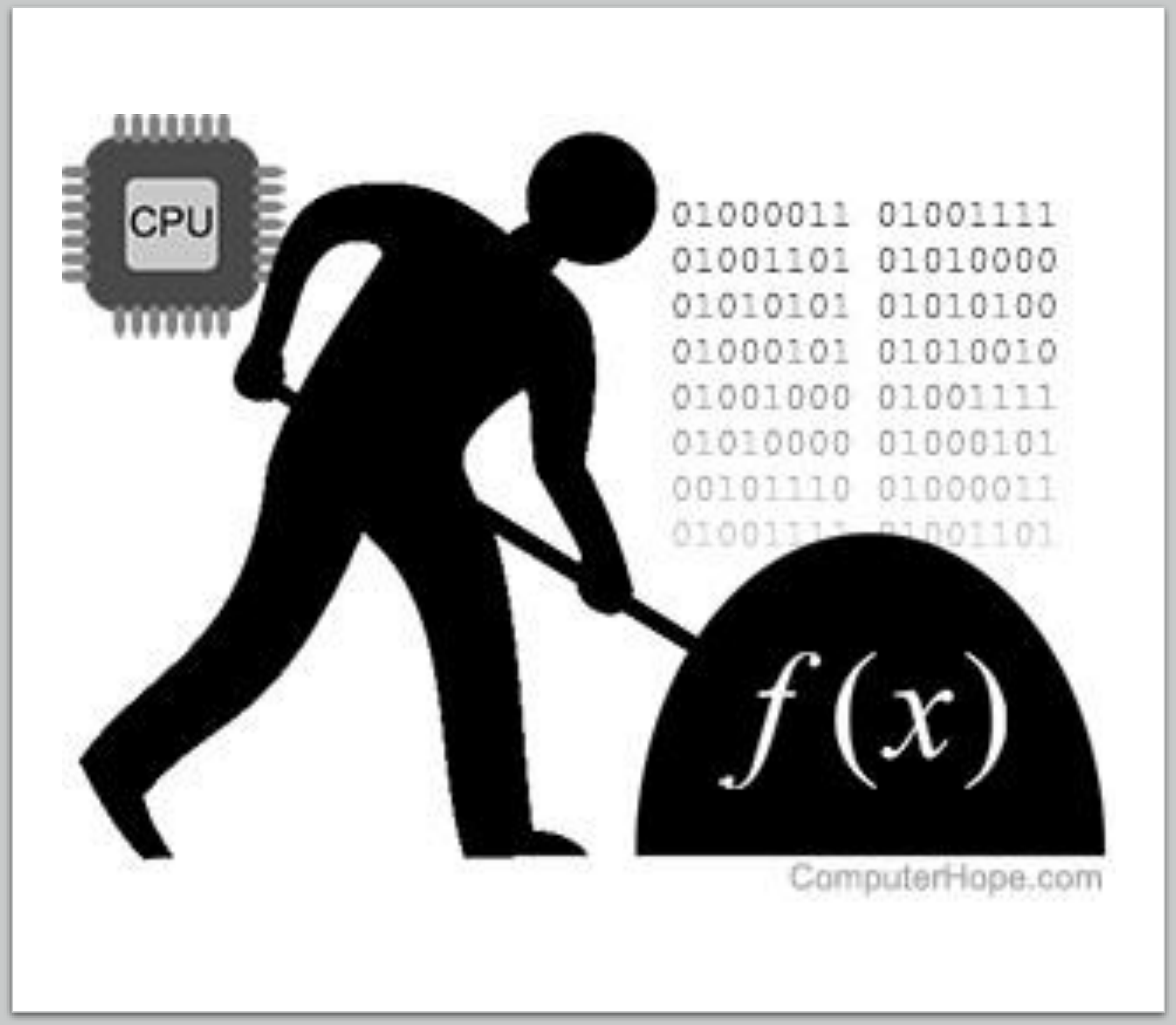
Practical Byzantine Fault Tolerance

Proof of Elapsed Time

Proof of Work

Principle: the more computing effort a node expends, the higher the chances that it will generate blocks.

The PoW consensus algorithm involves solving a computationally expensive calculation to add new blocks to the blockchain.



Proof of Work

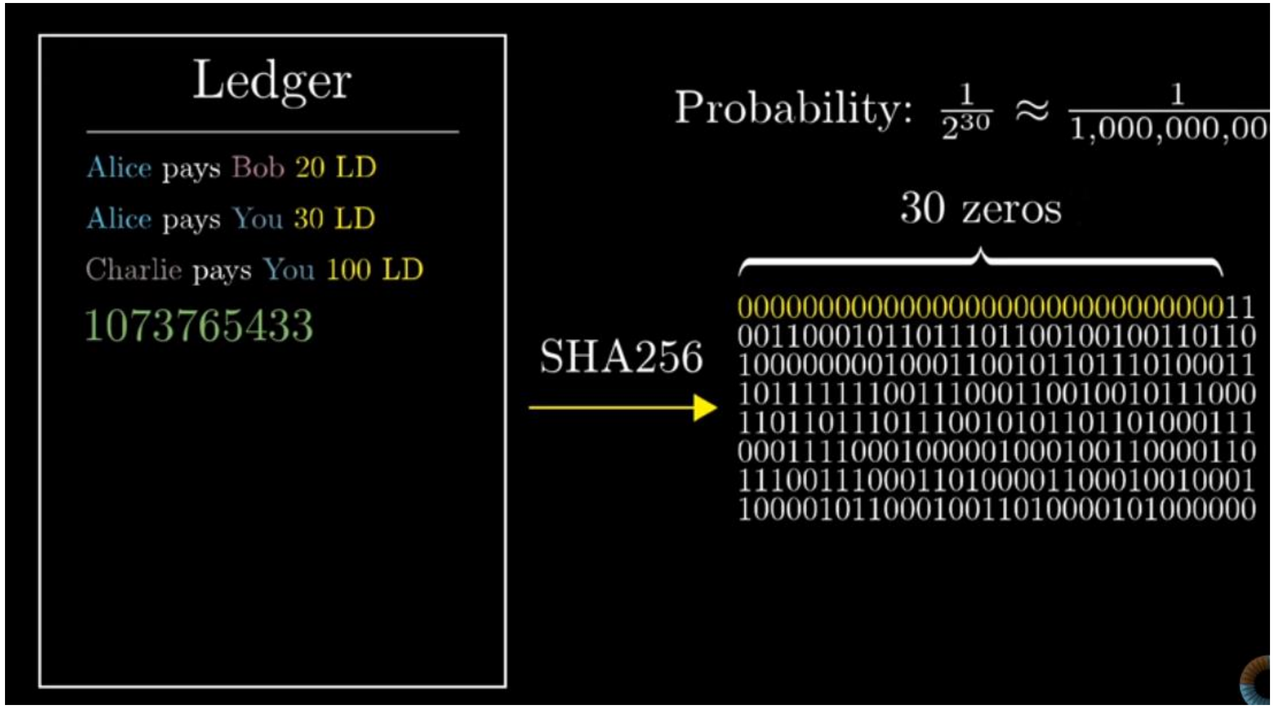
This process is also known as mining, and the nodes in the network that engage in mining are known as miners.

The incentive for mining transactions lies in economic payoffs, since competing miners are rewarded with coins as well as transaction fees

Proof of Work

To attach new blocks to the blockchain, a node must solve a math problem using trial and error.

The first participant to find a solution can distribute that solution and the block's entries to the network so other participants can build on the block



Ledger

Alice pays Bob 20 LD

Alice pays You 30 LD

Charlie pays You 100 LD

1073765433

SHA256

Probability: $\frac{1}{2^{30}} \approx \frac{1}{1{,}000{,}000{,}00}$

$\overbrace{000000000000000000000000000000}^{\text{30 zeros}}11$

```
00000000000000000000000000000011
00110001011011101100100100110110
10000000010001100101101110100011
10111111100111000110010010111000
11011011101110010101101101000111
00011110001000001000100110000110
11100111000110100001100010010001
10000101100010011010000101000000
```

Proof of Work

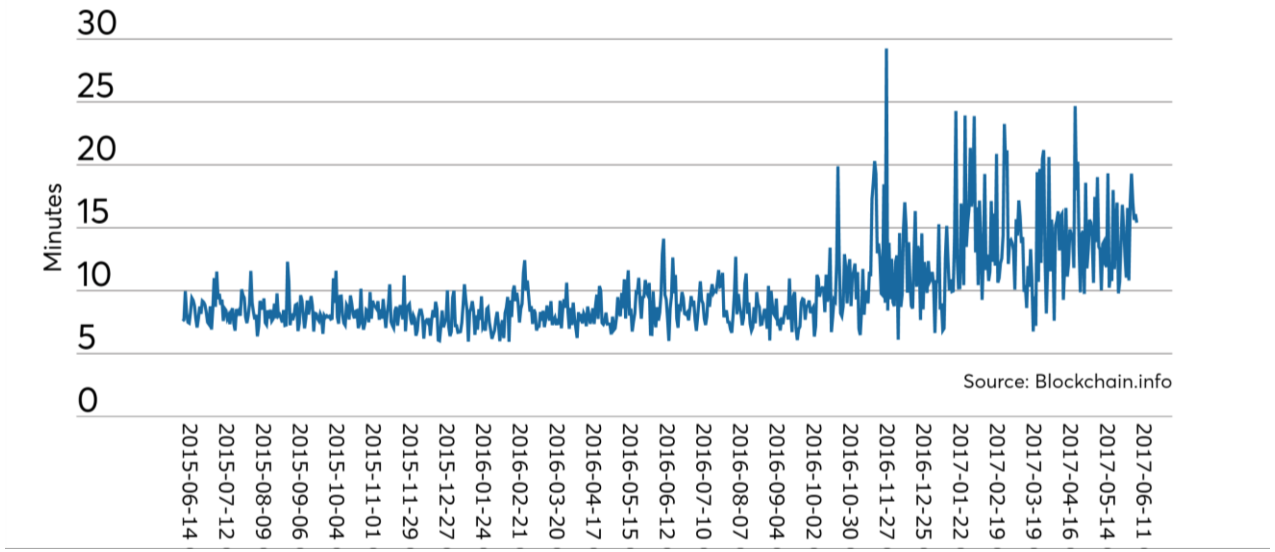
The PoW consensus mechanism requires significant energy to run, as a result, mining power is concentrated in countries where electricity is relatively cheap.

~57.6 TWh/YEAR
3iQ Research Group

Proof of Work

PoW has a high level of latency when it comes to transaction validation: it takes approximately 30 minutes from the time a payment instruction is sent to the time the payment originator can be sure that the transaction has been irreversibly made

This amount of time is long, especially compared to regular credit card transactions

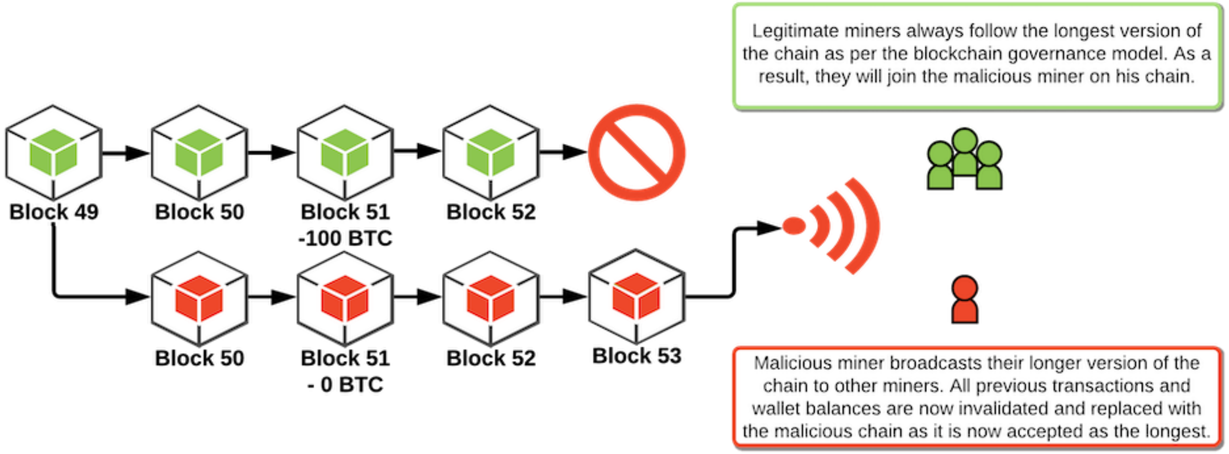


Source: Blockchain.info

Proof of Work

PoW is susceptible to the 51% attack by a group of miners that

control more than half of the network’s computing power



Legitimate miners always follow the longest version of the chain as per the blockchain governance model. As a result, they will join the malicious miner on his chain.

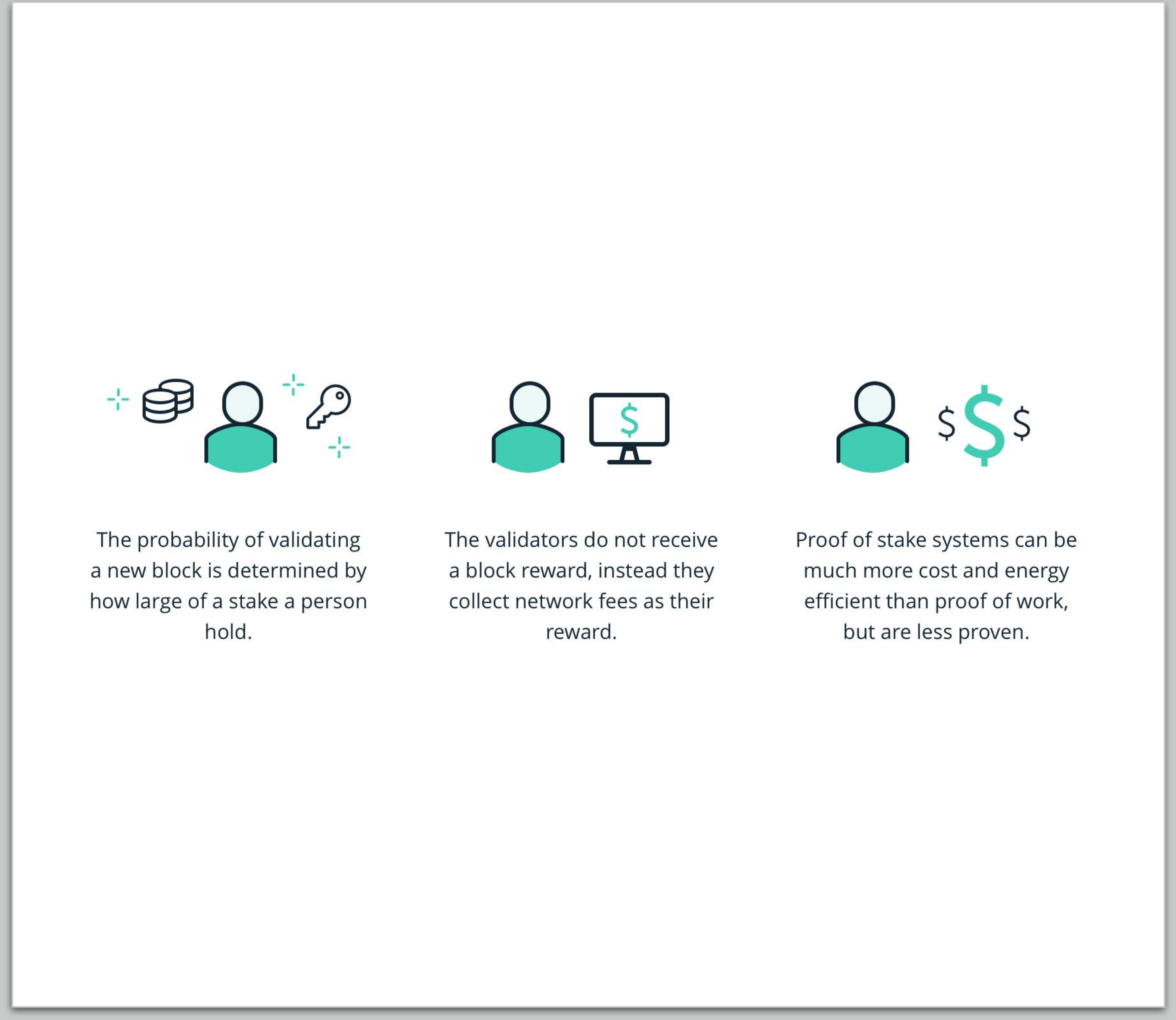
Malicious miner broadcasts their longer version of the chain to other miners. All previous transactions and wallet balances are now invalidated and replaced with the malicious chain as it is now accepted as the longest.

Proof of Stake

Principle: The higher the stakes of a node in the network, the greater the chances and the legitimacy of validating blocks.

With PoS, the nodes act as validators that confirm the transactions to earn a transaction fee

No traditional computing-based mining is required as inPoW; .



The probability of validating a new block is determined by how large of a stake a person hold.

The validators do not receive a block reward, instead they collect network fees as their reward.

Proof of stake systems can be much more cost and energy efficient than proof of work, but are less proven.

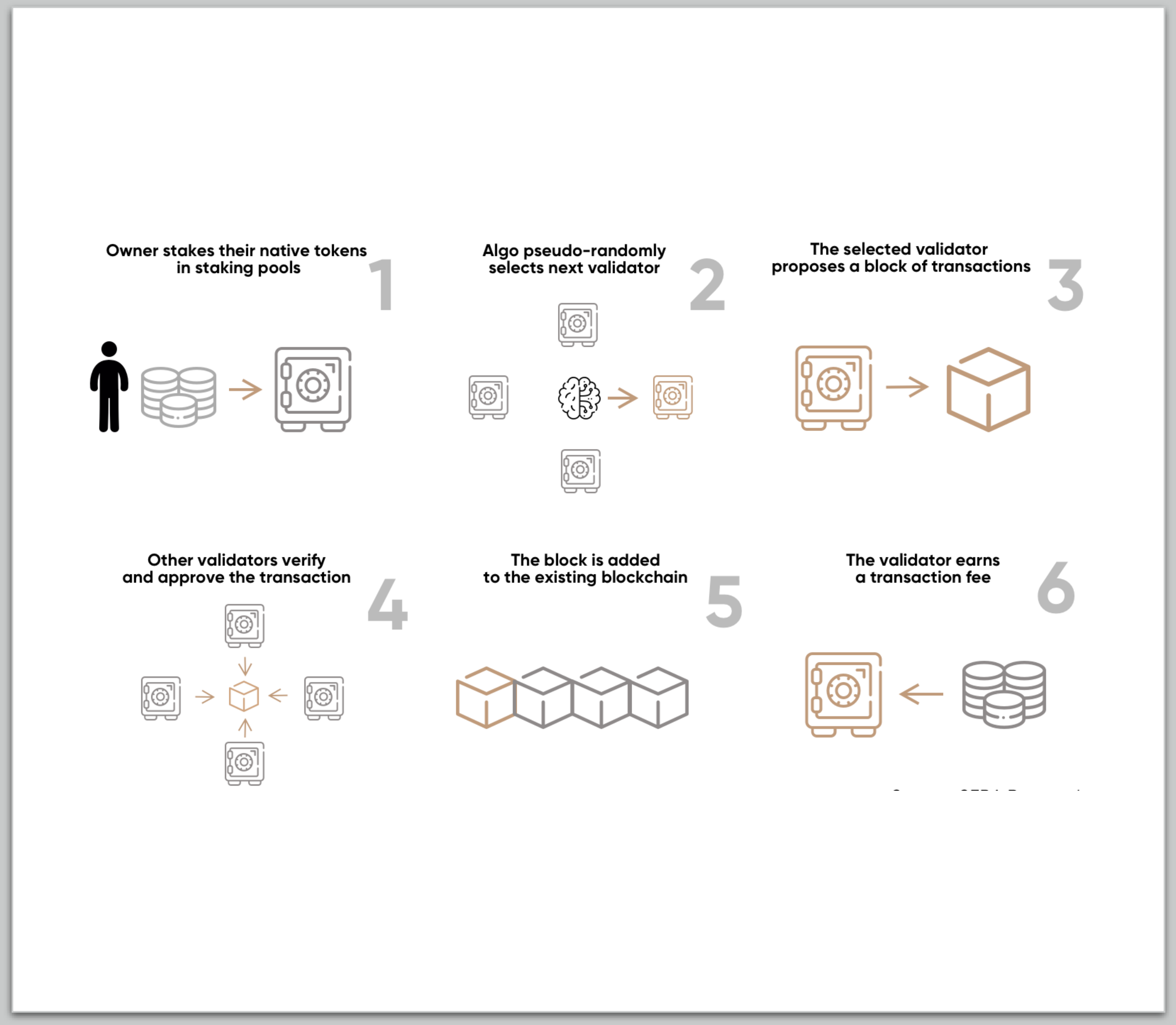
Proof of Stake

Nodes are randomly selected to validate blocks.

The probability that a node will be selected depends on the number of coins that it currently holds (stake): If node A stakes two coins and node B stakes one coin, node A is twice as likely to validate the next block of transactions

After the selection and validation process, the other node votes on whether to add the block

Note: The diagram shows Ethereum 2.0 implementation

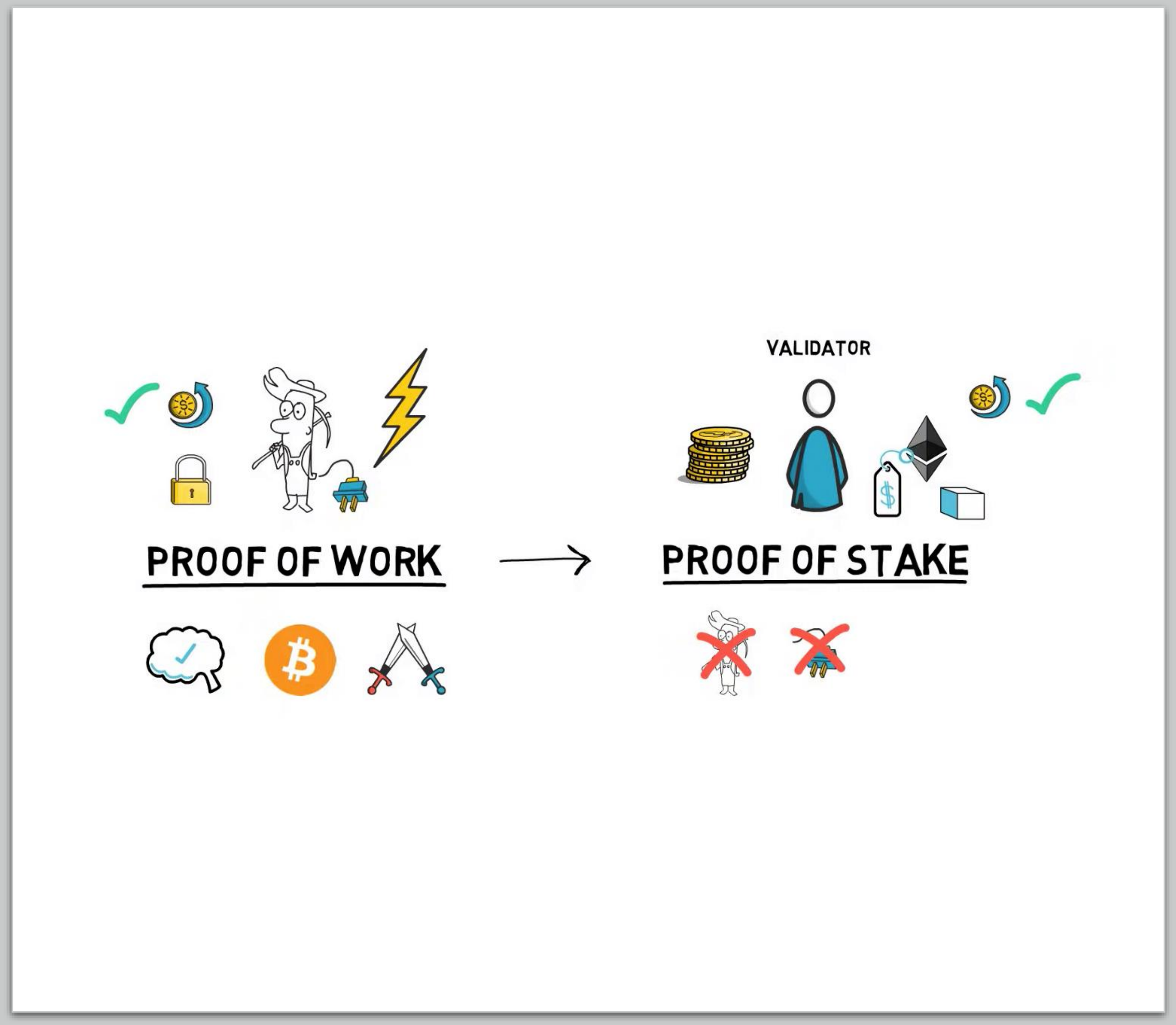

Owner stakes their native tokens in staking pools
1
Algo pseudo-randomly selects next validator
2
The selected validator proposes a block of transactions
3
Other validators verify and approve the transaction
4
The block is added to the existing blockchain
5
The validator earns a transaction fee
6

Proof of Stake

Advantages

PoS reduces the amount of electricity needed to validate transactions as for the case of PoW

PoS is less susceptible to 51% attack as the attackers already have more stake in the network



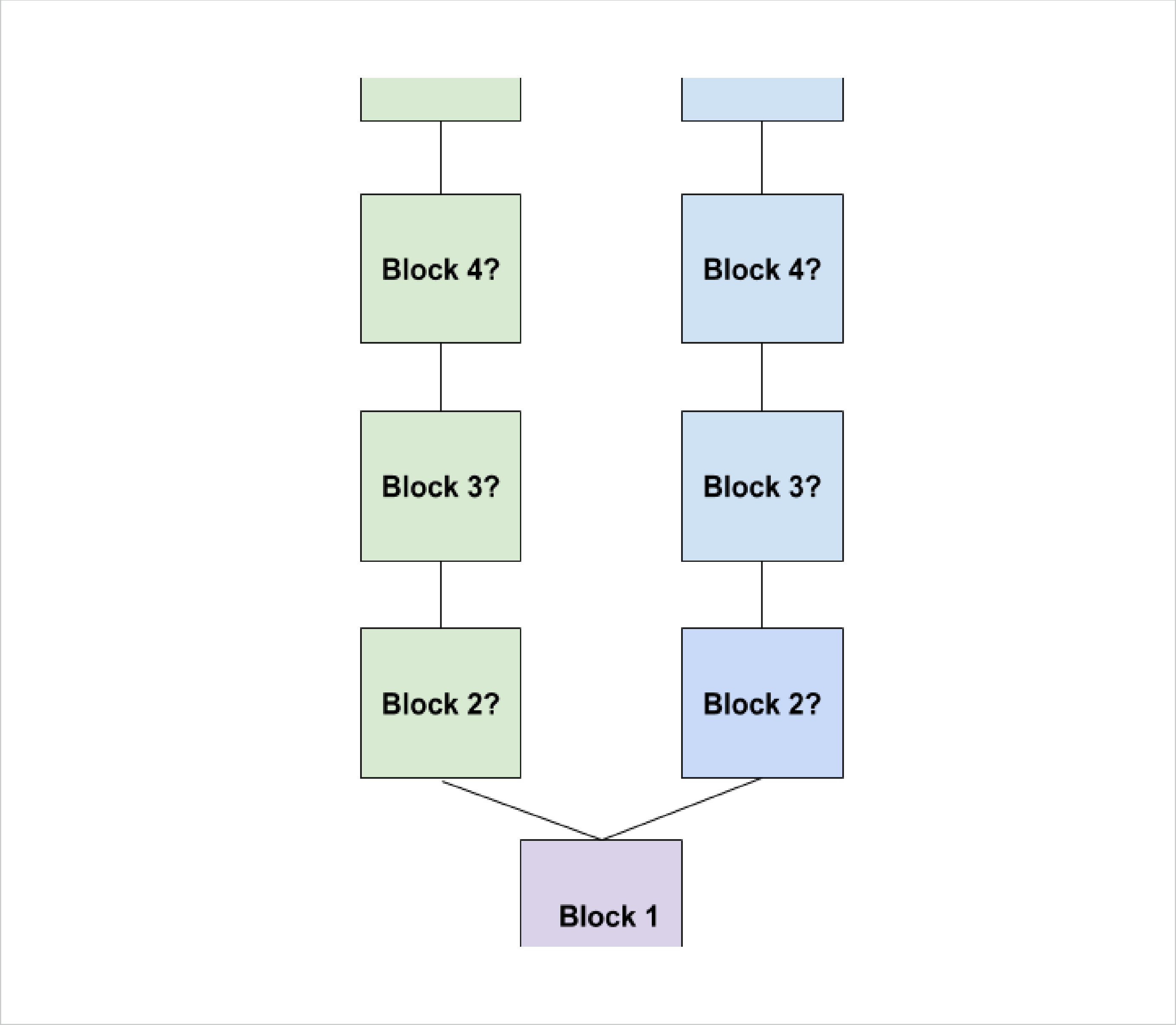
Proof of Stake

Downside

1. Nothing-at-Stake

Basic PoS algorithms face the Nothing-at-Stake problem, which arises because there are no direct costs for participating in the mining process

Validators mine on both chains to collect transaction fees on whichever fork ends up winning.



Proof of Stake

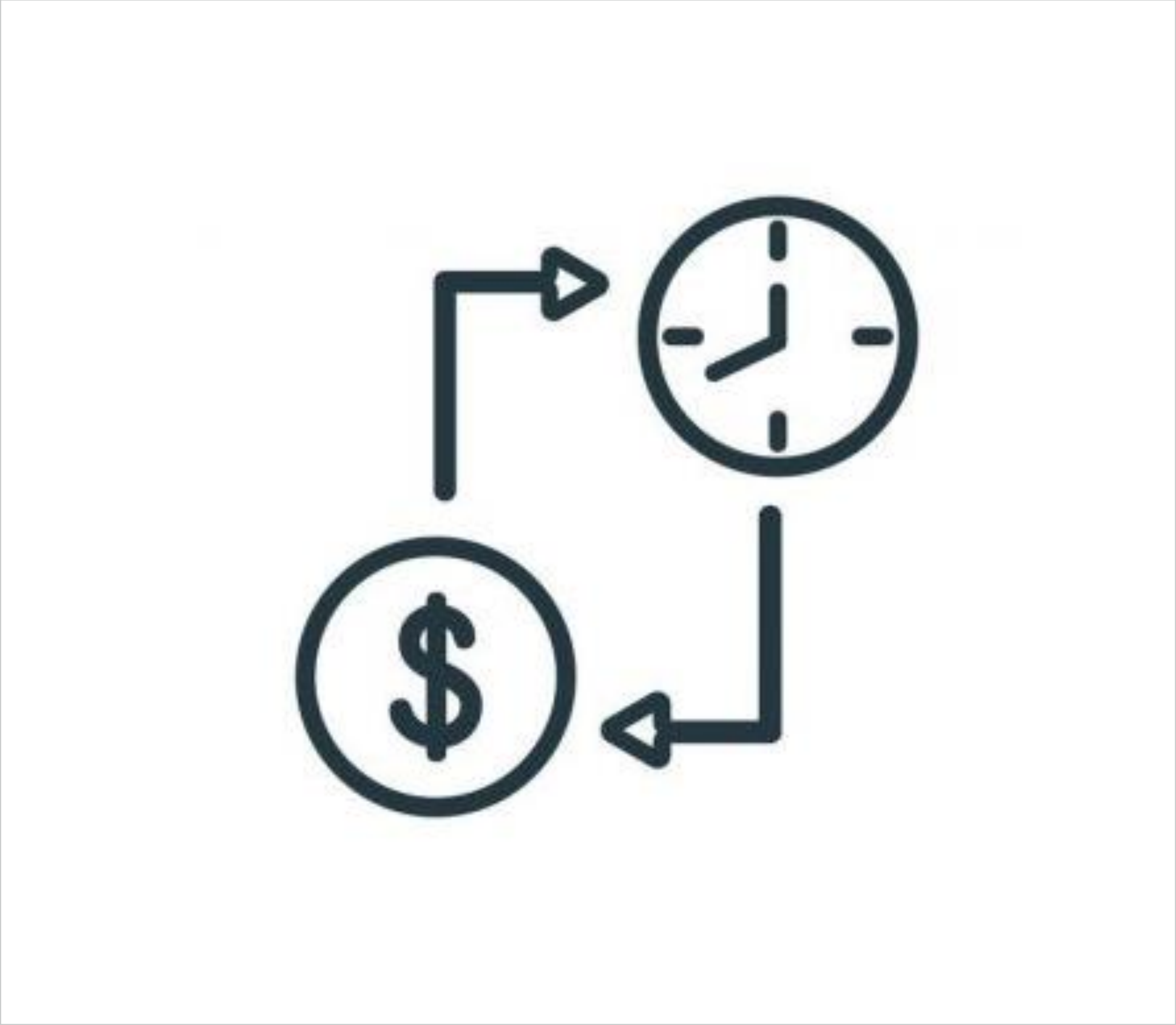
2. Attacks

Another dimension to this problem is a malicious actor who may not care about the economic costs but motivated to corrupt the network, such as may be the case with state-sponsored interference.

Proof of Capacity/Proof of Space

Principle: The more storage capacity a node expends, the greater the chance it will have to generate new blocks and be rewarded.

PoC is a resource-friendly alternative to PoW because it require miners to prove their commitment by staking storage space (i.e., disk capacity), rather than computing capacity



Proof of Capacity/Proof of Space

Instead of repeatedly guessing for the solution value as in a PoW system, PoC works by storing a list of possible solutions on the mining device's hard drive even before the mining activity commences.

The larger the hard drive, the more possible solution values one can store on the hard drive, the more chances a miner has to match the required hash value from his list, resulting in more chances to win the mining reward.

Proof of Capacity/Proof of Space

Step 1: Plotting

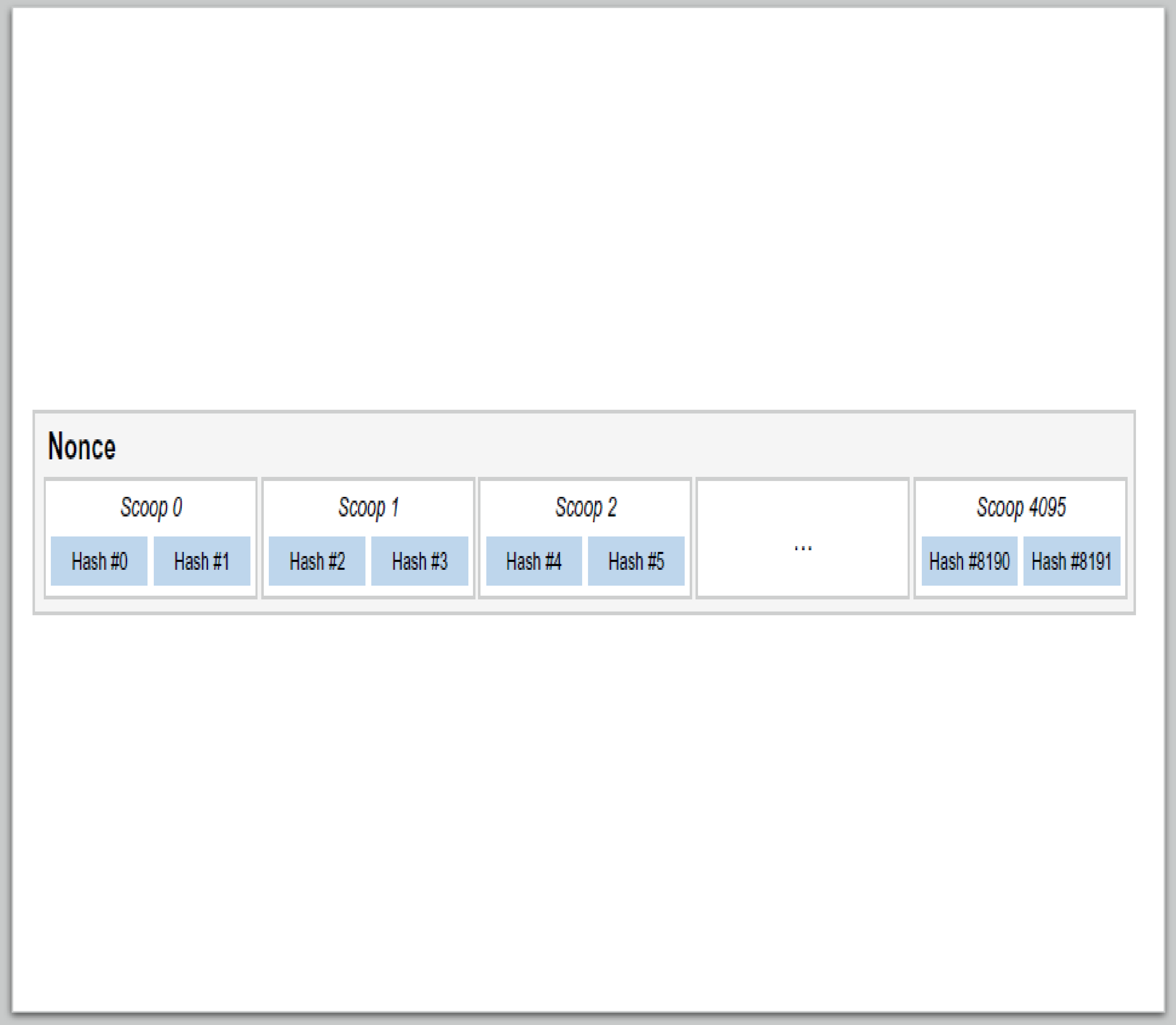
Plotting is the pre-computing and storing of hashes (solutions) by nodes before the actual mining process starts.

The solutions are hashes of random data including and includes miner Id.

The hashes are grouped into a scoop of 2 hashes

The scoops are grouped into nonces of 4096 scoops

Plotting is based on Shabal 256 hashing algorithm



Nonce

Scoop 0		*Scoop 1*		*Scoop 2*		...	*Scoop 4095*	
Hash #0	Hash #1	Hash #2	Hash #3	Hash #4	Hash #5		Hash #8190	Hash #8191

Proof of Capacity/Proof of Space

Step 2: Mining

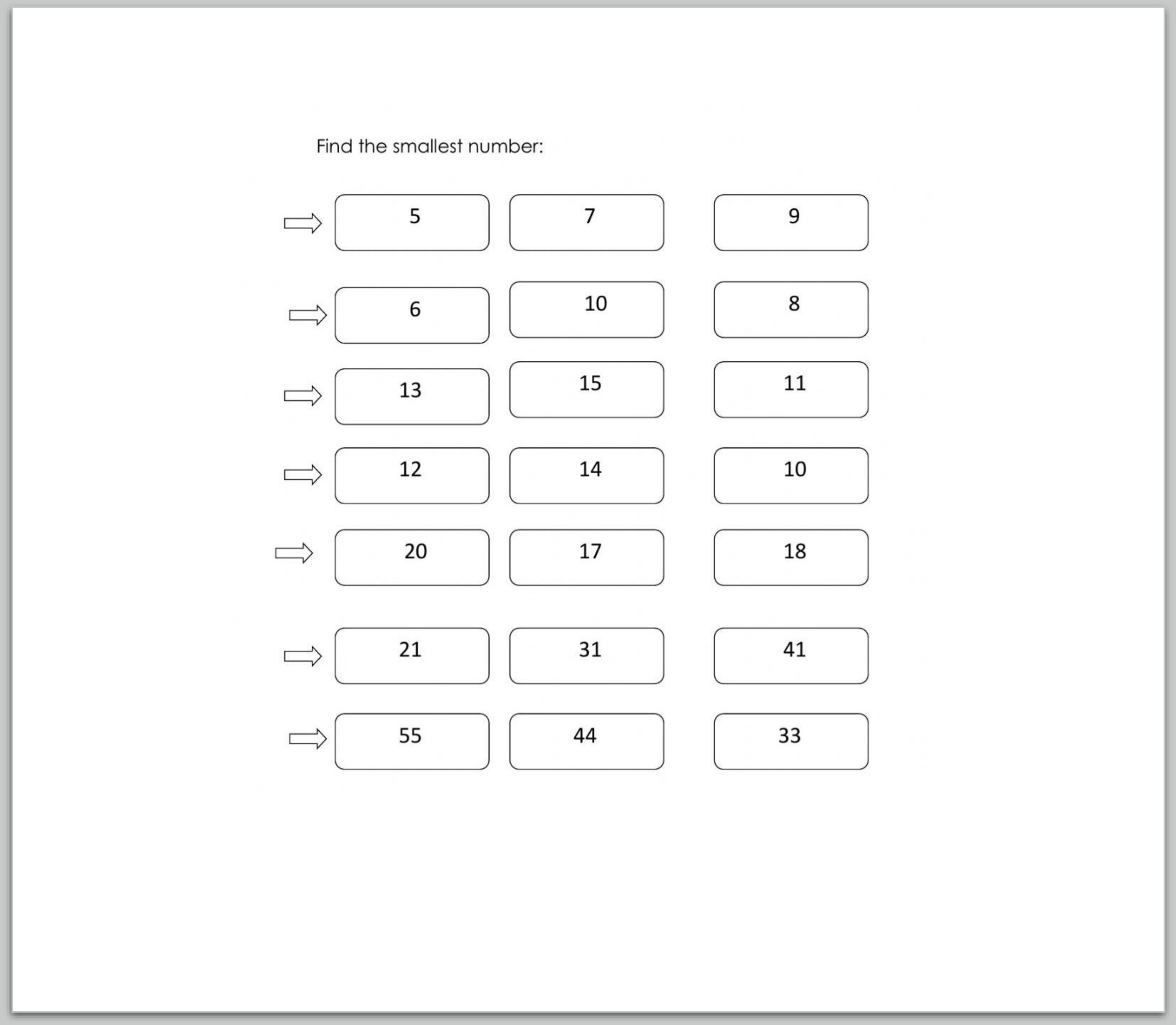
A miner node calculates/select a scoop number between 0 and 4095, say 50

Once the number is determined, the node will go to nonce 1 scoop 50 and utilize the data from that scoop to compute a number called deadline

The node then repeats this process for all the nonces in the plot file.

After calculating all the deadlines, the node chooses the shortest deadline, which is the number of seconds that elapsed between the forging of blocks.

If no one else has forged a block after this time has passed, the miner can forge a block and claim the block reward.



Find the smallest number:

⇨	5	7	9
⇨	6	10	8
⇨	13	15	11
⇨	12	14	10
⇨	20	17	18
⇨	21	31	41
⇨	55	44	33

Proof of Capacity/Proof of Space

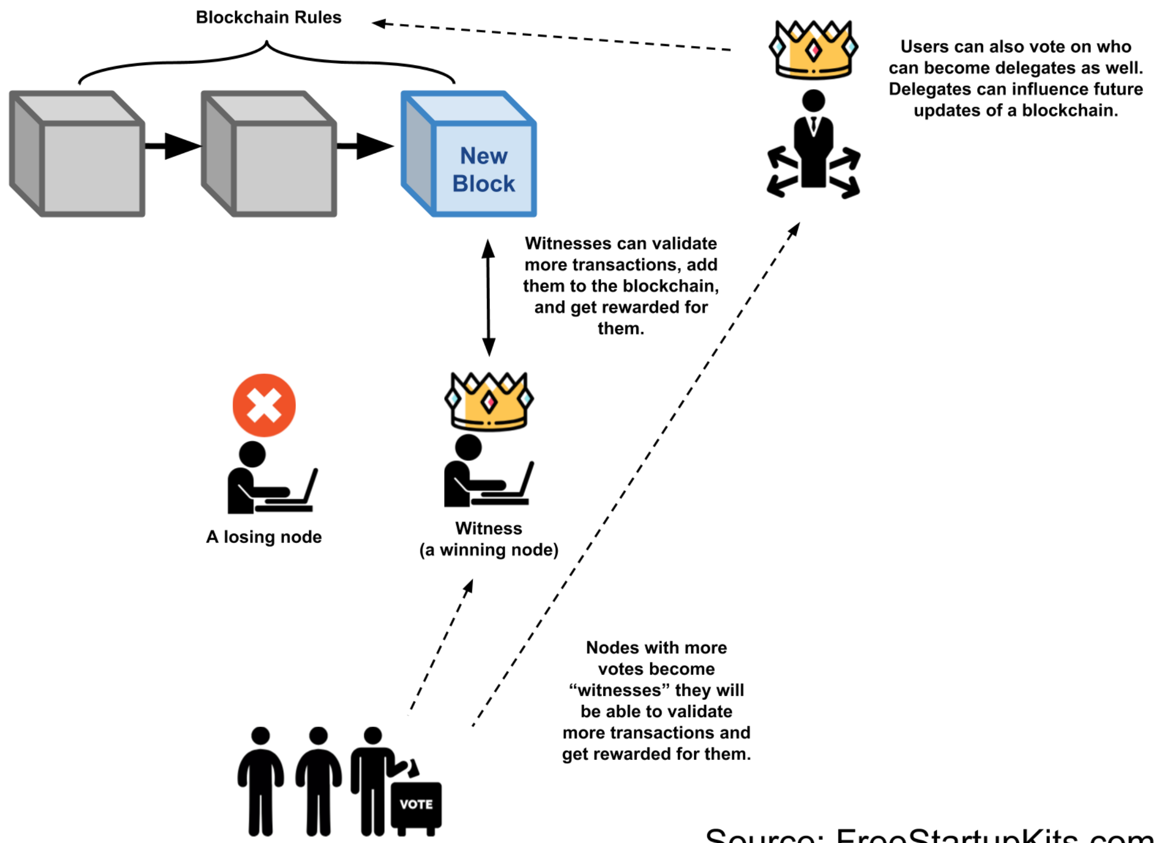
Blockchains that run on proof of capacity include Storj, Burst and Chia

Delegated Proof of Stake(DPoS)

Principle: The higher the stake of a validating node in the network, the more votes it can delegate to another trusted node to perform the validation.

DPoS is based on the concept of the “proof of stake.” The more the, the more voting rights. Network protection relies on a voting and election process

The actors in a DPoS system are called participants/voters, witnesses, and delegates.


Blockchain Rules
New Block
Users can also vote on who can become delegates as well. Delegates can influence future updates of a blockchain.
Witnesses can validate more transactions, add them to the blockchain, and get rewarded for them.
A losing node
Witness
(a winning node)
Nodes with more votes become “witnesses” they will be able to validate more transactions and get rewarded for them.
VOTE

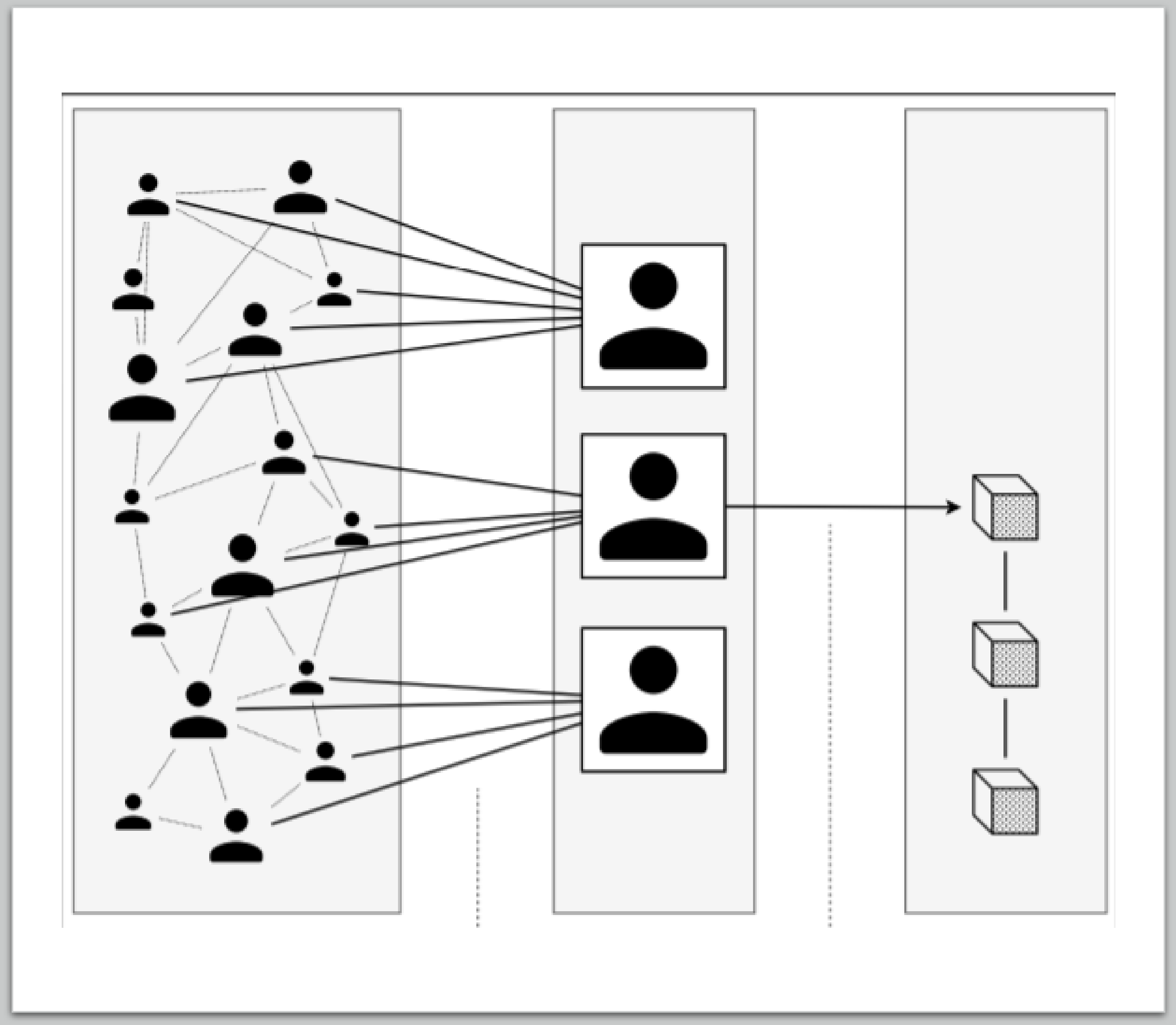
Source: FreeStartupKits.com

Delegated Proof of Stake(DPoS)

Witnesses are responsible for validating new blocks.

Witness receives rewards in terms of transaction fees and monthly payments.

Witness which underperforms are act unethically can be voted off during voting rounds.



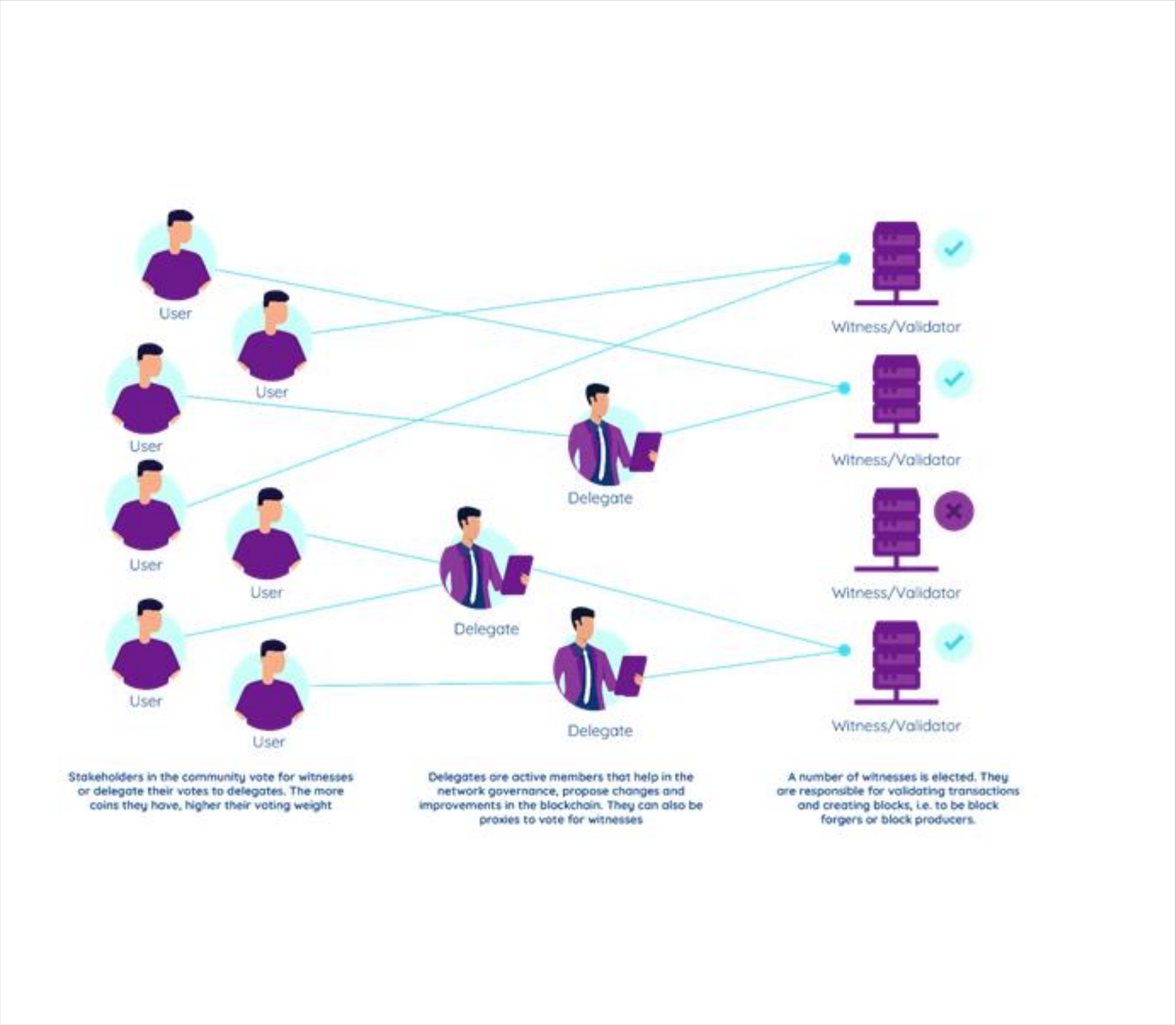
Delegated Proof of Stake(DPoS)

Delegates governs and regulate systems operations example submit proposals to change block size or witness fees.

The proposals are again voted by participants

Delegates do not validate transactions

Examples of cryptocurrencies that use DPoS include Lisk, EOS, and BitShares.



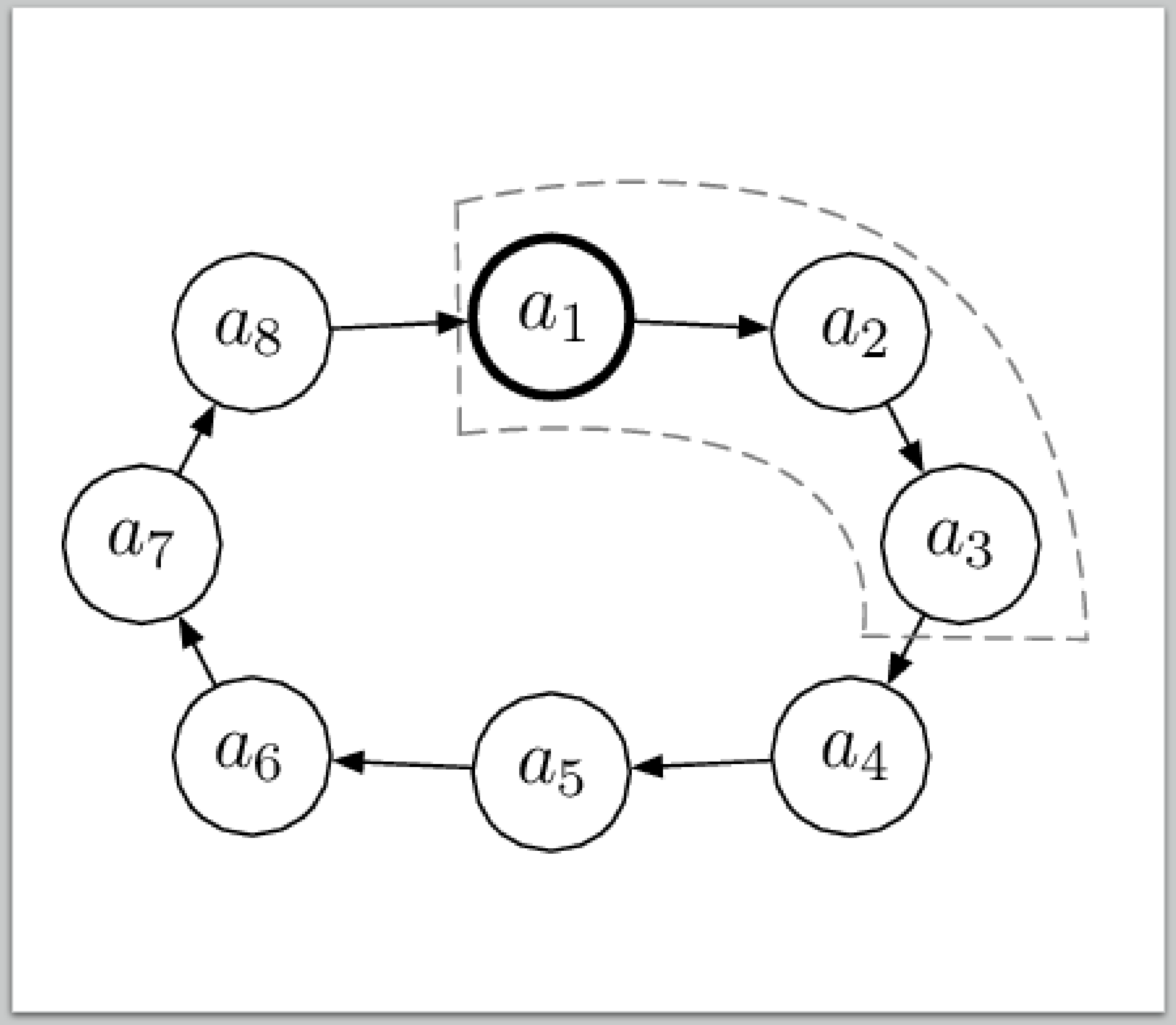
Stakeholders in the community vote for witnesses or delegate their votes to delegates. The more coins they have, higher their voting weight

Delegates are active members that help in the network governance, propose changes and improvements in the blockchain. They can also be proxies to vote for witnesses

A number of witnesses is elected. They are responsible for validating transactions and creating blocks, i.e. to be block forgers or block producers.

Proof of Authority

- Principle: A select set of N established participants hold elevated authority in the network.
- Any participant with such authority can propose the next block, and if a subset of participants signs the block, it is added to the blockchain.
- Unlike all the other consensus mechanisms, PoA is considered to be non-democratic and can be used for permissioned ledgers



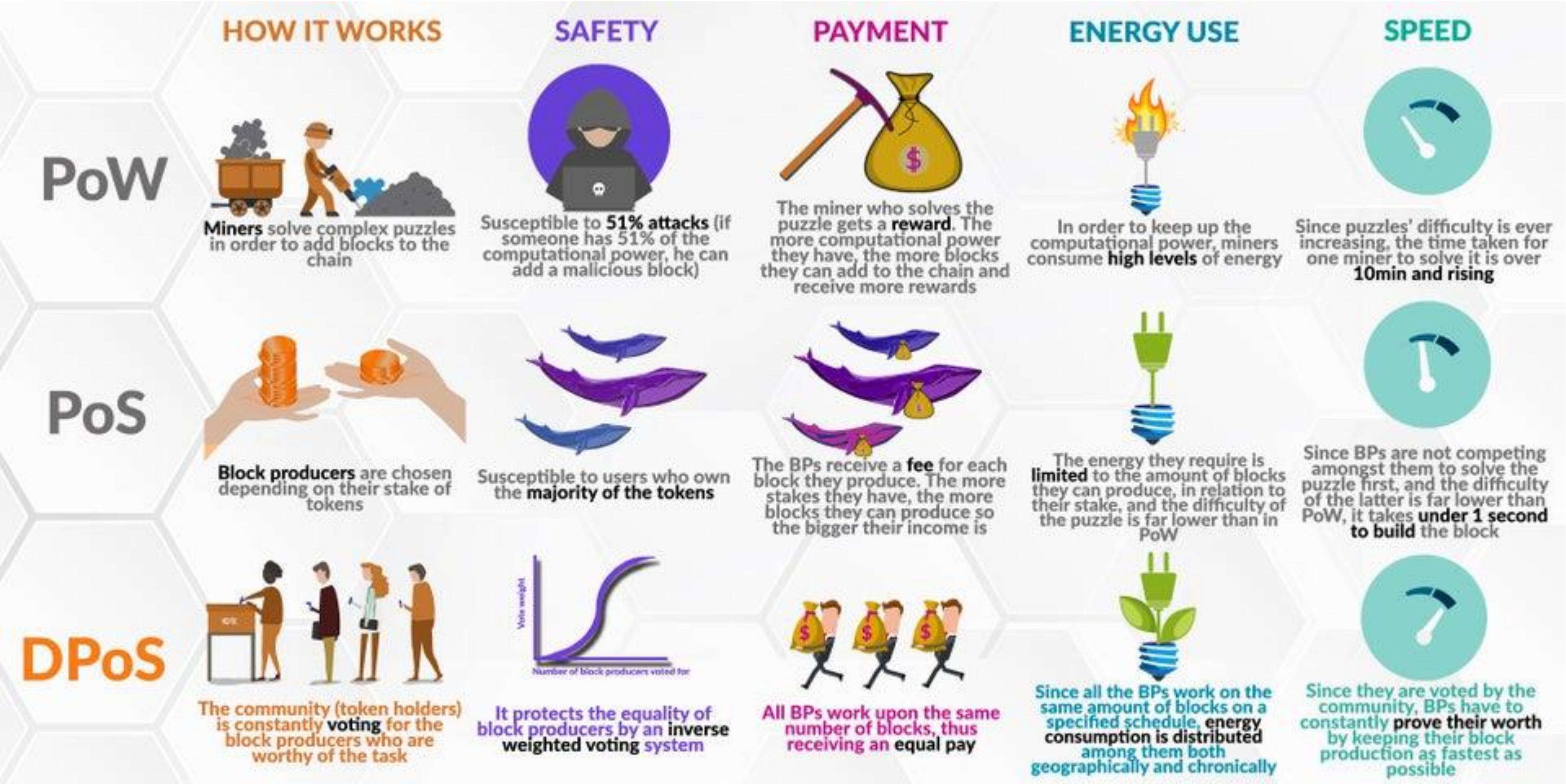
Proof of Authority

- The mechanism centers on the use of “authorities,” which are designated nodes that can create new blocks and secure the ledger.
- Each authoritative node must provide its public key so their activities can be tracked in the network

Proof of Authority

The best-known examples of the use of a PoA consensus mechanism today are the two Ethereum test-nets, Kovan and Rinkeby.

Summary


Vote weight
Number of block producers voted for

	HOW IT WORKS	SAFETY	PAYMENT	ENERGY USE	SPEED
PoW	**Miners** solve complex puzzles in order to add blocks to the chain	Susceptible to **51% attacks** (if someone has 51% of the computational power, he can add a malicious block)	The miner who solves the puzzle gets a **reward**. The more computational power they have, the more blocks they can add to the chain and receive more rewards	In order to keep up the computational power, miners consume **high levels** of energy	Since puzzles' difficulty is ever increasing, the time taken for one miner to solve it is over **10min and rising**
PoS	**Block producers** are chosen depending on their stake of tokens	Susceptible to users who own the **majority of the tokens**	The BPs receive a **fee** for each block they produce. The more stakes they have, the more blocks they can produce so the bigger their income is	The energy they require is **limited** to the amount of blocks they can produce, in relation to their stake, and the difficulty of the puzzle is far lower than in PoW	Since BPs are not competing amongst them to solve the puzzle first, and the difficulty of the latter is far lower than PoW, it takes **under 1 second to build** the block
DPoS	The community (token holders) is constantly **voting** for the block producers who are worthy of the task	It protects the equality of block producers by an **inverse weighted voting** system	All BPs work upon the same number of blocks, thus receiving an **equal pay**	Since all the BPs work on the same amount of blocks on a specified schedule, **energy consumption is distributed** among them both geographically and chronically	Since they are voted by the community, BPs have to constantly **prove their worth** by keeping their block production as fastest as possible

Activity: Set up PoA Blockchain