

# **Proof of Work and Proof of Stake**

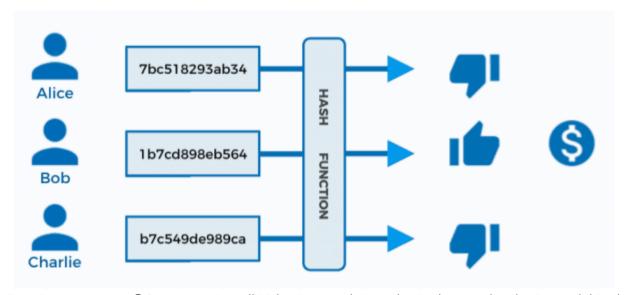


#### **Proof of Work**

- Proof of Work is the consensus algorithm where miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.
- Some of the problems included with Proof of Work are:
  - Hash function how to find the input knowing the output.
  - Integer factorization how to present a number as a multiplication of two other numbers.
  - Guided tour puzzle protocol If the server suspects a DoS attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it's a 'how to find a chain of hash function values' problem.
- Miners receive a reward when they solve the complex mathematical problem.
- For example in Bitcoin miners receive 12.5 bitcoins for solving the puzzle.
- Miners can also receive transaction fees in addition to rewards.



### **Proof of Work**



Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited



#### **Proof of Stake**

- Proof-of-Work algorithm rewards miners who solve complex mathematical problems with the end goal of validating transactions and creating new blocks. On the other hand, in the Proof-of-Stake algorithm, the creator of a new block is chosen in a deterministic way, depending on its wealth/stake in the blockchain.
- No block reward
- All the digital currencies are created at the start of the chain, and their number never changes. Miners only take the transaction fees.



### **Proof of Stake**

#### Proof of stake



The blocks are validated as per the stake held by the person over the Blockchain.



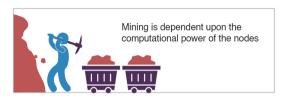
Miners/Validators only collect the transaction fees as per the stake.

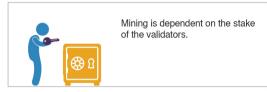


There is no complex computation involved that's why they are more efficient then proof of work systems

## greatlearning Learning for Life

#### **Proof of Work Proof of Stake** VS







Miners receive block rewards with transaction fees for quessing the value of nonce.



Miners don't receive block rewards. only transaction fees are distributed to miners.



Nobody can modify the blockchain until and unless they have more than 51% power of the complete blockchain.



Attackers require 51% or greater stake on blockchain to take over blockchain, the cost is very high compared to the POW 51% attack.



## Thank You