Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

Proofs(Consensus Algorithms) in Blockchain

PoW – Proof-of-Work

Proof-of-Work

- Miners has to solve a crypto puzzle
- Miner who solved the puzzle first, will get the mining reward.
- There is a lot of power consumption in PoW
- Higher you have the hash rate or hashing power, higher the chance to mine the block
- Miners are also group together to increase the hashing power and distribute the mining reward, called mining pools

Energie usage ⏫

Mining pools -> centralization 😡

Drawback of PoW

PoS – Proof-of-Stake

PoS – Proof-of-Stake

Instead of Miners, PoS has **Validators**

Validators are responsible for minting/forging the block(s)

To become a validator, a node has to deposit certain amount of coins into the network as **Stake**

We can think it like a security deposit

PoS – Proof-of-Stake

Size of Stake determines the chances of validator to be chosen to forge the next block

No electricity wastage, No mining pools,

Brings Disadvantages too (favors rich nodes, 51% attack(less chances than PoW))

Casper – Proof-of-Stake system by Ethereum – Deployed on Ethereum testnet

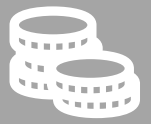
Cardano project is developing proof-of-stake Algorithm, Ouroboros

Delegated Proof-of-Stake

Proof-of-Authority

Proof of **Burn**

A consensus algorithm in which miners burn coins in order to get right to update the blockchain/ or mine a block



Verifiers also need to burn the coins in order to validate the transactions