What is consensus?

- Agreement on a single truth
- Blockchain systems use consensus mechanisms to achieve agreement on a single data value or a single state of the network among distributed systems.
- Many different types of consensus algorithms
  - POW (proof of work)
  - POS (proof of stake)
  - POA (proof of authority)
  - DPoS (Delegated Proof of Stake)
  - BFT (Byzantine Fault Tolerance)
  - DAGs (Directed Acyclic Graphs)

Proof of Work

- Proof-of-Work system requires its users to perform some form of work to participate
- The work needs to be difficult for the client but easy for the server / network to verify
- Miner nodes compete to ‘solve a Block’ or group transactions together, and have that block accepted onto the blockchain

Proof of Stake

- Proof of Stake is an alternative to validate transactions and achieve the necessary distributed consensus
- Like PoW, its an algorithm with the same purpose but the process to reach the goal is quite different
- Creator of a new block is chosen in a deterministic way
  - Depends on its wealth, or STAKE
- No block reward
  - Take the transaction fees

PROOF OF WORK

The probability of mining a block depends on the amount of work a miner does

Takes more energy than Proof of Stake

One example is Mining, which uses computer cycle time to validate new transactions

Stakeholders validate new blocks by utilizing their share of coins on the network

The first example of Proof of Stake was Peercoin

A user would need to own a majority of all coins in order to attack the network

PROOF OF STAKE

COMPARING PROOF ALGORITHMS

Proof of work & Proof of stake are methods of verifying the authenticity of transactions, without the need for a centralized third party.

WHAT ARE THEIR MAIN DIFFERENCES?

HolyTransaction

Proof of Authority

- Leverages identity as the form of stake rather than actually staking tokens
- Identity is staked by a group of validators (authorities)
- Validators are pre-approved to validate transactions and blocks
  - The validator group tends to be small (~25 or less)
  - Ensures efficiency and manageable security on the network
- Low requirement of computational power
- No requirement of communication between nodes to reach consensus