Day 3 Blockchain Notes

Blockchain Consensus Mechanisms:

Consensus mechanisms ensure that all participants in a blockchain network agree on the current state of the ledger. There are various types of consensus mechanisms, each with its own advantages and disadvantages.

- **Proof of Work (PoW)**: In PoW, miners solve complex mathematical puzzles to validate transactions and add them to the blockchain. This process requires a large amount of computational power and electricity, making it energy-intensive.

Example: Bitcoin uses PoW, where miners compete to solve a cryptographic puzzle. The first miner to solve the puzzle gets to add a block to the blockchain and is rewarded with Bitcoin.

- **Proof of Stake (PoS)**: PoS is an alternative to PoW. In PoS, validators are selected to create the next block based on how much cryptocurrency they hold and are willing to "stake" as collateral. This method is more energy-efficient than PoW.

Example: Ethereum 2.0 uses PoS, where validators are selected based on the amount of Ethereum they hold and are incentivized to act honestly by the amount they stake.

- **Delegated Proof of Stake (DPoS)**: DPoS is a variation of PoS where stakeholders vote for a limited number of delegates who are responsible for validating transactions. This reduces the number of validators needed, making the process faster.

Example: EOS uses DPoS, where token holders vote for delegates who validate transactions

and secure the network.

- **Proof of Authority (PoA)**: PoA is a consensus mechanism used in permissioned blockchains. In PoA, validators are pre-approved and trusted entities responsible for validating transactions.

Example: In supply chain management, PoA can be used to validate transactions among trusted parties, like manufacturers, distributors, and retailers.

- **Practical Byzantine Fault Tolerance (PBFT)**: PBFT is a consensus mechanism used in permissioned blockchains. It allows for consensus even if some nodes in the network are faulty or malicious.

Example: Hyperledger Fabric uses PBFT to ensure agreement between nodes in the network, even if some nodes are malicious.