ASSIGNMENT 01

1. Difference between public and private and consortium blockchain.

Public: This blockchain is a permissionless, non-restrictive, distributed ledger system, which means anyone who is connected to the internet can join a blockchain network and become a part of it. The basic use of such blockchain is for exchanging cryptocurrencies and mining.

Private: Private blockchain is a permission and a restrictive blockchain that operates in a closed network. Such blockchain is mostly used within an organization where only particular members are participants of a blockchain network.

Consortium: Consortium blockchain is best suited for organizations where there is a need for both types of blockchains, i.e., public and private. In this type, there is more than one central in-charge, or we can say more than one organization involved who provides access to pre-selected nodes for reading, writing, and auditing the blockchain. Since there is no single authority governing the control, it maintains decentralized nature.

Features	Public	Private	Consortium
Accessibility	Anyone	Single Person/ Central Incharge	More than one central in-charge.
Who can join?	Anyone	Permissioned and known identities	Permissioned and known identities
Consensus Mechanism	PoS/PoW	Voting or multi-party consensus algorithm	Voting or multi-party consensus algorithm
Transaction Speed	Slow	Lighter & Faster	Lighter & Faster
Decentralization	Completed Decentralized	Less Decentralized	Less Decentralized

2. Merkle Trees w.r.t. Blockchain:

Merkle trees are also called hash trees. Every leaf node in a merkle tree is labelled with a crypto hash of a data block and every non leaf node is labelled with the crypto hash of labels of child node. Merkle trees allow efficient and secure storage in a blockchain. They can help ensure that data blocks received from other peers in a peer-to-peer network are received undamaged and unaltered, and even to check that the other peers do not lie and send fake blocks.

3. Double Spending in Blockchain.

Double spending means the expenditure of the same digital currency twice or more to avail the multiple services. It is a technical flaw that allows users to duplicate money. Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user's wallet is not secured.
Suppose a user wants to avail of services from Merchant 'A' and Merchant 'B'.
The user first made a digital transaction with Merchant 'A'.
The copy of the cryptocurrency is stored on the user's computer.
So the user uses the same cryptocurrency to pay Merchant 'B'
Now both the merchants have the illusion that the money has been credited since the transactions were not confirmed by the miners.

4. Difference between PoS & PoW.

Proof of Stake	Proof of Work
Block creators are called validators	Block creators are called miners
Participants must own coins or tokens to become a validator	Participants must buy equipment and energy to become a miner
Energy efficient	Not energy efficient
Security through community control	Robust security due to expensive upfront requirement
Validators receive transactions fees as rewards	Miners receive block rewards