

Assignment 1

D	D	M	M	Y	Y	Y	Y

Q1] Considering the different type of Block chain (Public, private, consortium) discuss consensus protocol. (POS & POW) vary in their implementation. What are potential advantages & disadvantages of them.

⇒ ☉ Public Block chain.

POW: Ideal for open permissionless network like Bitcoin. It offers strong security due to its high computational cost making it difficult to tamper with it, but its slow in transaction processing.

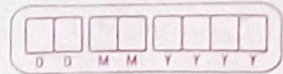
POS: It's faster and more energy-efficient than POW but might be susceptible to attack if a large stake holder colludes with others, security is also a concern in its immature state.

☉ Private Block chain

POW: less common due to its resource-intensive nature.

Private block chain often have a known set of participants, making POW's security feature less necessary.

POS: Suitable for private block chain, it's faster and more scalable, aligning well with the permissioned environment where trusted participants are involved.



① Consortium Blockchain

Both PoS and PoW are viable; the choice depends on the specific needs of the consortium. PoW can be used for added security, while PoS offers better scalability.

Q2] Merkle tree plays a crucial role in structure of Blockchain. Explain how Merkle trees enhance the efficiency and security of Block chain network. How do they compare to other data structure approaches used in distributed system.

⇒ Efficiency:

Merkle trees allow efficient verification of transactions within a block. Each transaction has a unique hash and these hashes are combined into a single merkle root hash stored in the block header. By verifying the merkle root, anyone can confirm if a specific transaction exists within the block, without downloading the entire block.

Secure and Tamper free

Hashing: Each node in the Merkle tree is a hash of its child nodes, creating a hierarchical structure.



Tamper detection : Any change in the data will alter the hash at the leaf node which will propagate up the tree and change the merkle root. This makes it easy to detect tampering.

Comparison with other data structures

Linked List : LL are simple but inefficient for verifying large sets of transactions. Merkle trees provide a more structured and efficient way.

Hash table : They do not inherently support hierarchical structure and are less effective for providing the inclusion of an item without additional data.

Binary Search tree : While BST are efficient for some operation, they are not optimized for cryptographic verification and proof of integrity.