Deep Salunkhe
21102A0014

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 it's high computational cost making it difficult to tamper with it, but it's slow in transaction processing

PoS: It's faster and more energy-efficient than PoW but might be su susceptible to attack if a large stake holder colludes with other, security is also concern in it's immature state.

⊙ Private Block chain

PoW: less Common due to it's 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 participant are involved.

Deep Salunkhe
2102A00124

D D M M Y Y Y Y

⊙ Consortium Block chain

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 offer 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

⇒ Effiriency :

Merkle trees allow efficient verification of transactions within a block. each transaction has a unique has and these hashes are combined into a single merkle root has 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 it's child nodes, creating a hierarchical structure.

Deep Selvakumar
2302A00114.

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 structure.

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.