L5 SOD A&B

BLOCKCHAIN HOMEWORK

To be submitted on Monday

Q1: True or False

i. The Ethereum Virtual Machine (EVM) is responsible for executing smart contracts on the Ethereum network.
ii. Blockchain transactions are stored in a linear sequence within blocks.
iii. Public keys are used to encrypt transactions, while private keys are used to decrypt them.
iv. Blockchain technology can only function in a centralized environment.
v. A Sybil attack involves a malicious actor creating numerous fake identities to disrupt a network.

Q2: Multiple Choice

i. Which of the following is a core principle of blockchain?
a) Centralization
b) Immutability
c) Inflation
d) Secrecy

ii. What is the primary purpose of a Merkle Tree in a blockchain?
a) It ensures the immutability of blockchain data.
b) It cryptographically links blocks together in the chain.
c) It allows for efficient verification of transactions within a block.
d) It encrypts private key information.

iii. Which of these is a known vulnerability in smart contracts?
a) Routing Attack
b) Reentrancy Attack
c) Selfish Mining
d) Eclipse Attack

Q3: Fill in the Blanks

i. A _____ is a cryptographic data structure used to verify transactions efficiently in blockchain systems.
(Block / Merkle Tree / Private Key)

ii. In a blockchain, the _____ is used to verify the ownership of an address, while the _____ is used to sign transactions.
(Public Key / Private Key / Smart Contract)

iii. The _____ consensus mechanism is energy-efficient and is used in Ethereum 2.0.
(Proof of Work / Proof of Stake / Proof of Authority)

iv. A _____ attack occurs when a malicious node monopolizes communication between a targeted node and the rest of the network.
(Eclipse / Sybil / Selfish Mining)

v. In blockchain, the _____ ensures the chronological and linear order of blocks.
(Private Key / Consensus Mechanism / Encryption)

vi. A smart contract is _____ stored on the blockchain that runs automatically when predefined conditions are met.
(Public Key / self-executing code / Blockchain)

vii. In a Hierarchical Deterministic Wallet, _____ are used to generate a sequence of keys.
(Consensus Mechanism / Mnemonic Seeds / Smart Contracts)

Q4: Matching
Match the Blockchain Consensus Mechanism in **Column B** with its key characteristic in **Column C**.

Column A	Column B	Column C
1.....	a) Proof of Work (PoW)	1. Relies on a voting system where selected nodes validate blocks.
2.....	b) Proof of Stake (PoS)	2. Miners solve computational puzzles to validate blocks.
3.....	c) Delegated Proof of Stake (DPoS)	3. Validators are chosen based on the amount of stake they hold.
4.....	d) Proof of Authority (PoA)	4. Validators are chosen based on reputation and identity.
		5. Uses trusted execution environments to randomly assign validation slots.

		6. Selects validators based on network activity and contribution.

Q5: Comparative Analysis
What are the advantages and disadvantages of using a public blockchain compared to a private blockchain?

Q6: Explanation
Explain the role of Ethereum's Peer-to-Peer (P2P) network in ensuring the decentralization and security of the blockchain.

Q7: Explanation
How does the InterPlanetary File System (IPFS) improve the efficiency and scalability of data storage for blockchain systems?

Practical Assessment

Q8: Design and Explanation
Draw and explain the architecture of a blockchain-based supply chain system that integrates with third-party services like payment gateways. Your diagram and explanation should clearly show the flow of goods, payments, and data throughout the system.