MANIPAL INSTITUTE OF TECHNOLOGY
BENGALURU
*(A constituent unit of MAHE, Manipal)*

**SURPRISE TEST**
**VII-SEMESTER (CSE Core)**
**BLOCKCHAIN-TECHNOLOGY (CSE_4533)**

**Duration: 30-minutes**

| Student name | Reg no. | Section | Semester |
|---|---|---|---|
| | | | |

| Q NO. | Question | Marks |
|---|---|---|
| **Q1** | Question:<br>A tech startup, **FreeVoice**, is building a decentralized social media platform where users can post content to a blockchain-like system. The system has the following requirements:<br>It must be massively scalable to handle millions of user actions (likes, posts, comments) per second.<br>It does not need traditional blockchains or global consensus on every transaction.<br>Users should only validate the parts of the ledger they care about, without relying on global consensus.<br>The system should maintain eventual consistency while still preventing double spending or spam-like behaviors.<br>To achieve this, FreeVoice decides to adopt a DAG-based architecture using implicit consensus, where every new transaction indirectly confirms previous ones.<br>Which of the following best describes how implicit consensus works in a protocol like the one FreeVoice uses?<br><br>A. Transactions are grouped into blocks, and miners compete to validate them by solving computational puzzles.<br>B. A rotating set of validators reach consensus on each block through multiple rounds of voting.<br>C. Each transaction references and confirms previous transactions, forming a DAG structure where consensus emerges from accumulated validations.<br>D. Validators explicitly agree on a global state through a finality gadget in Proof-of-Stake (PoS). | **1M** |
| **Q2** | **The five elements of blockchain are distribution, encryption, immutability, tokenization and**:<br>A. Transparency<br>B. Authorization<br>C. Efficiency<br>D. Decentralization | **0.5M** |
| **Q3** | What does Byzantine Fault Tolerance (BFT) refer to in distributed systems?<br>A. Capacity to process thousands of transactions per second.<br>B. Integration with Internet of Things devices<br>C. The ability to reach consensus despite malicious or failing nodes<br>D. Automatic private key rotation | **0.5M** |
| **Q4.** | After widespread complaints about Scrooge's favouritism in ScroogeCoin, a group of developers forces the idea and launches Bitrust a decentralized cryptocurrency.<br>BitTrust uses<br>A public ledger (Blockchain Proof-of-Work consensus protocol, Digital signatures for transaction authorization, UTXO (Unspent Transaction Output) model for coin ownership, Support for basic smart contracts through locking/unlocking scripts.<br>In BitTrust, transactions are validated by miners and included in blocks. Each transaction Input must reference a previous unspent output, and each is signed by the owner's private key. A developer named Eve writes a smart contract that releases coins to anyone who can solve a puzzle. The script says:<br>"Pay 1 BitTrust Coin to whoever provides a preimage of the hash h." | **1M** |

| | | |
|---|---|---|
| | This is a valid locking script.Eve publishes the contract, and several users face to find the preimage Mallory , a miner, finds the correct preimage and includes it in a transaction, and spending the contract and sending the coin to herself , but instead of broadcasting the transaction immediately, she waits and mines the next block block privately, including her Winning transaction<br>At the same time , Alice also finds the preimage and creates a valid transaction spending the same contract output, which gets broadcast to the network and included in a block by overtakes the public chain , making Alice's transaction invalid.<br>**Questions:**<br>A. Mallory's action is invalid because Alice's transaction was signed and published first.<br>B. Digital signatures alone cannot resolve conflicts in distributed ledgers the chain with The most accumulated work determines the accepted history<br>C. Smart contract prevents miners from exploring timing issues because they enforce execution order.<br>D. Mallory's block is rejected because double spending cannot occur once a transaction is signed | |
| **Q5** | Based on the previous question, the Bit Trust community debates what went wrong, Many M developers argue that Eve's smart contract was "**trustless**" because it used code to automatically reward the first person who provided the correct solution<br><br>However, some security researchers point out a **design flaw**<br>Even though Alice **solved the puzzle fairly** and **broadcast her transaction**, the fact that the smart contract lacked any **timing or ordering mechanism** allowed Mallory (a miner) to Alice's solution, copy it, and **include her own identical solution first in a private block**<br>This raises an important question about **front-running**, **transaction ordering**, and the limits of **on-chain trustless logic.** To prevent this in the future, the community proposes adding **timing constraints** to smart contracts, such as:<br>• "Only accept this solution if it arrives before timestamp T"<br>• "Only allow address X to claim the reward for the first N blocks"<br>**Question**:<br>What is the **core limitation** that allowed Mallory, the miner, to front-run Alice's solution and win the reward, despite Alice broadcasting her transaction first?<br>A. The smart contract failed to use digital signatures, allowing unauthorized spending<br>B. The smart contract relied only on the correctness of the solution, without considering transaction origin or network order.<br>C. The Proof-of-Work algorithm was too slow to process transactions in real time.<br>D. Alice forgot to sign her transaction, so the network could not verify her solution | **1M** |
| **Q6** | What is the security incident when attackers gain control over the blockchain network resources?<br>A. Reentrancy attack<br>B. 51% attack<br>C. Brute force attack<br>D. Invasion attack | **0.5M** |
| **Q7** | Under what condition is an orphan block most commonly created in a blockchain?<br>A. When a 51% attack is successful<br>B. When two miners solve a block simultaneously<br>C. When a node goes offline permanently<br>D. When all transactions are invalid | **0.5M** |

| **Questions.** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| **Answers.** | C | D | C | B | B | B | B | Error | Error | Error |