VIT
Vellore Institute of Technology

Course: BCSE326L - Blockchain Architecture Design
Class NBR(s): 2128
Time: Three Hours
Slot: E2+TE2
Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions
(10 X 10 = 100 Marks)

1. How blockchain layers and features can enhance transparency and prevent fraud in a supply chain, focusing on the roles of the propagation and semantic layers?

2. a) How the block header components help us to ensure integrity and linkage between blocks in a blockchain? [5]

   b) If a blockchain block uses a SHA-256 hash and the target difficulty requires a hash to start with four leading zeros, estimate how many nonce values might be tested before a valid hash is found. What role does the nonce play in this process? [5]

3.a) I. How nodes in a blockchain network decide which chain of blocks to accept when multiple chains exist? [5+5]

II. A blockchain network has two competing chains: Chain A has a total difficulty of 150, and Chain B has a total difficulty of 180. Which chain will the nodes accept, and why?

OR

3.b) I. Describe the lifecycle of a blockchain transaction from creation to confirmation. What steps ensure its validity? [5+5]

II. A user wants to send 1.2 BTC. They use two inputs: one bitcoin worth of 0.7 BTC and another bitcoin worth of 0.6 BTC. If the transaction fee is 0.05 BTC, how much change will be returned to the user?

4. Explain the process of block propagation in a blockchain network. How does it ensure that all nodes receive the newly mined block efficiently?

5.a) Write a Python script using the Bitcoin Core JSON-RPC API to send Bitcoin to a given address and retrieve the transaction details. Specify the RPC commands used, include proper error handling and comments in your code.

OR

5.b) Suppose you are developing a lightweight Bitcoin application using BTCD. How would you design the system to handle blockchain synchronization and transaction verification? Also explain, how BTCD operates compared to Bitcoin Core?

6. Compare hardware wallets with software and mobile wallets in terms of security architecture. What makes hardware wallets more resistant to attacks?

7. Create a Solidity contract with a function to store a user's email address and another function to retrieve it. Demonstrate its functionality using Remix.

8. Analyse, how colored coins extend the functionality of Bitcoin beyond currency transactions? What limitations do they inherit from the Bitcoin protocol?

9. Evaluate the effectiveness of using blockchain for storing and sharing electronic medical records. What are the trade-offs between data privacy, accessibility, and interoperability?

10. Design a model for a blockchain land registry system that uses scrypt for consensus. How would the system ensure tamper-proof ownership history and transparent access for governmental and legal auditing?

⇔⇔⇔ E/E/TY ⇔⇔⇔