

(3 Hours)

(Total Marks: 80)

- N.B.:**
1. Question No. 1 is compulsory.
 2. Answer any three out of the remaining questions.
 3. Assume suitable data if necessary.
 4. Figures to the right indicate full marks.

- Q1. Attempt the following (any 4):** (20)
- a. Define blockchain? Compare different types of blockchain.
 - b. What is a smart contract? How crowdfunding platforms can be managed using smart contracts?
 - c. What is a backup in Practical Byzantine Fault Tolerance (PBFT) algorithm?
 - d. What is a Merkle tree? Explain the structure of a Merkle tree.
 - e. Write a program in solidity to check whether a number is prime or not.
- Q2. Attempt the following:**
- a. State and explain various challenges that occur while implementing blockchain. (10)
 - b. What is a double spending problem? How PoW solves the problem of double spending? (10)
- Q3. Attempt the following:**
- a. Compare Bitcoin and Ethereum. How to calculate Mining difficulty in bitcoin (10)
 - b. Explain Hyperledger Fabric v1 architecture. (10)
- Q4. Attempt the following:**
- a. Describe the architecture of Ethereum. (10)
 - b. Write a program in solidity to implement multi-level inheritance. (10)
- Q5. Attempt the following:**
- a. Explain PAXOS consensus algorithm for a private blockchain. (10)
 - b. Explain fixed and dynamic arrays in solidity with suitable examples. (10)
- Q6. Write short notes on (any 2):** (20)
- a. Corda
 - b. UTXO model of Bitcoin
 - c. Quorum
 - d. Fallback function in Solidity
