

Roll Number: \_\_\_\_\_

**Thapar Institute of Engineering & Technology, Patiala**

Computer Science & Engineering Department

EST

B.E. (Final Year): Semester- VII (2023/24)

Course Code: UCS754,

Course Name: Blockchain Technology and Applications

December 04, 2023

Monday, 2:00– 5:00 Hrs

Time: 3 Hours, M. Marks: 35

Name Of Faculty: Dr. Neeraj Kumar

**Note: Do any seven questions from the set of eight questions in the paper.**

- |     |  |             |
|-----|--|-------------|
| Q1. | a) You are a car seller/buyer broker company say <i>Car24.com</i> providing various services to the end users? Create a smart contract using solidity for online tracking of car maintenance, history of services, buyer/seller information, police verification, current market value, original owner/series of buyers and sellers. Use appropriate data structures for identity verification, and tracking of all the above information during design of the smart contract in solidity. | (2.5+2.5)   |
|     | b) How hash functions are used by miners to mine the blocks for checking valid or invalid transaction to be part of a block? How immutability and repudiation is preserved keeping in view of the denial of claim for an asset?  |             |
| Q2. | a) Why there is a requirement of GasValue for Transaction execution in smart contract? What is the difference between memory arrays and storage arrays?  | (1.5+1.5+2) |
|     | b) How identity verification of an individual has been identified in large number of nodes? How scalability of the transactions is evaluated on Blockchain networks?   |             |
|     | c) Design a smart contract for maintaining an asset in an online commodity management with reference to demand (D) and supply (S) at various company stores separated at N number of locations around the globe.   |             |
| Q3. | a) What are <i>chaincode</i> used in Hyperledger Fabric? How transactions are validated using in Hyperledger Fabric? Draw the labeled architecture diagram of Hyperledger Fabric with respect to transactions read and write operations?   | (2.5+2.5)   |
|     | b) What is the role of membership service providers in Hyperledger Fabric? Explain <i>Endorsement, Signature, and Hash-based policies</i> for transaction verification?  |             |
| Q4. | a) Explain PBFT Consensus algorithm? What are the various phases in its operations? How fault tolerance is achieved in PBFT implementation? What are limitations of PBFT algorithm?  | (2.5+2.5)   |
|     | b) Differentiate between Web2.0 and Web3.0 with respect to transaction speed, accuracy and security?   |             |
| Q5. | a) Explain the delegated proof of stake consensus algorithm used in the blockchain for verification and validation of transactions? How stake is maintained in this algorithm?   | (2.5+2.5)   |
|     | b) Explain Merkle root hash tree construction for verification of transactions? How it is computed and used in different blocks in the blockchain networks?  |             |
| Q6. | a) Differentiate between blockchain and hashgraphs with respect to transaction processing time, accuracy, speed and security. Also, list applications of hashgraph in comparison to the blockchain?  | (2.5+2.5)   |
|     | b) How IoTa tangle is different with Bitcoin? What are the potential applications of IoTa tangle in comparison to Bitcoin and Ethereum?  |             |
| Q7. | a) Explain the process of creating decentralized applications (dApps) using truffle framework.   | P.T.O       |

- b) Create a smart contract for supply chain management (SCM). SCM involves multiple parties, such as suppliers, manufacturers, distributors, retailers, and consumers, who need to exchange information, money, and products. Using smart contracts, record transaction and movement of goods and track on a shared ledger that is visible and verifiable by all participants, which can increase trust, accountability, and traceability in the supply chain. Additionally, execute predefined actions based on predefined conditions, such as releasing payments, transferring ownership, or triggering alerts, which can reduce manual errors, delays, and fraud, as well as save time and resources. (2.5+2.5)
- Q8. a) Create a simple smart game contract that allows a player to stake ETH and the pool is shuffled and any random player to win the round and as soon as a winner emerges a new pool begins. In each pool, the record of the number of winners, losers, and total number of players need to be maintained using appropriate storage management. (2.5+2.5)
- b) Explain integer overflow attack and 51% attack in solidity language.