

B.TECH.
(SEM VI) THEORY EXAMINATION 2022-23
BLOCKCHAIN ARCHITECTURE DESIGN

Time: 3 Hours**Total Marks: 100****Note:** Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt all questions in brief. 2 x 10 = 20

- (a) Give the formal definition of Blockchain.
- (b) Classify the different types of Blockchain.
- (c) Examine this statement-“suppose an adversary (or malicious user) wants to change the transaction of one block.” If s/he is successfully change it then what are consequences occurred due to the this modification?
- (d) Describe “Mining” procedure used in Public Blockchain.
- (e) Define the term “Channels” used in the Hyper-ledger fabric.
- (f) List down the properties of Smart Contracts.
- (g) List down the Pros and Cons of using Blockchain in the Trade/Supply Chain System.
- (h) In PBFT consensus algorithm, if the number of byzantine nodes is 5, then find out the number of honest nodes and total number of nodes present in the blockchain network.
- (i) Define Private and Public Key Cryptography.
- (j) Examine the security mechanism utilized in the Blockchain.

SECTION B

2. Attempt any three of the following: 10x3=30

- (a) Describe the centralized, decentralized and distributed system architecture. Also give a brief comparison among these three architecture based on their unique properties.
- (b) What is the consensus algorithm? Explain the basic requirements for consensus protocol.
- (c) Discuss Hyper-ledger Fabric. How do we decompose the consensus process?
- (d) Discuss the public distribution system (PDS). Also, discuss the utilization of blockchain in PDS with respect to the centralized PDS.
- (e) Given the Elliptic curve $E_{11}(1,6)$ with the coordinate $G(2,7)$. Find out the $(2*P)$.

SECTION C

3. Attempt any one part of the following: 10x1=10

- (a) Define Merkle trees. Explain the use of Merkle tree in blockchain in detail.
- (b) Suppose you have eight data points (or eight transactions)- 8 to 1. Create the Merkle tree for the given set of transactions ordered from 8 to 1 and then compute the in-order, pre-order, and post-order traversal for the created Merkle tree.

4. Attempt any one part of the following: 10x1=10

- (a) Define hash functions. Also, discuss the characteristics and applications of hash functions.

- (b) Explain Proof-of-Work (PoW) consensus algorithm used in the public blockchain.

5. Attempt any *one* part of the following:

10x1=10

- (a) Describe the Practical Byzantine Fault Tolerance (PBFT) consensus model adopted in Hyper-ledger Fabric.
- (b) Create the smart contract for withdrawal and deposit functionality of banking application using the modifier.

6. Attempt any *one* part of the following:

10x1=10

- (a) The current Financial Software System (FSS) utilizes the centralized platforms to perform the customer's transactions. As a developer, if we shift from centralized system to decentralized system, then list down the advantages and disadvantages of the decentralized FSS. Also, Justify your answer with the support of your argument.
- (b) Now-a-days the blockchain technology is considered as trusted approach for different applications like supply chain management system. This technology achieves data immutability and provides the transparent system. Is it possible that blockchain technology can be used to completely removes the fraud and corruption from the present public and private sectors? Provides your observation on it.

7. Attempt any *one* part of the following:

10x1=10

- (a) Describe the concept of "Digital Signature" used in the blockchain.
- (b) Discuss Blockchain for Government with respect to Digital identity, land records and other kinds of record keeping between other government entities. Is it safe? Justify your answer.