E/G/TY

Reg. No:

VIT
Vellore Institute of Technology

Summer Term Final Assessment Test – July 2025

Course: **CSI3013** - **Blockchain Technologies**

Class NBR(s): **0462**

Slot: **F1+TF1+F2+TF2**

Time: **Three Hours**

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. Explain the block mining process in the Bitcoin blockchain. Describe how miners select transactions, construct the block, compute the proof-of-work, and broadcast the block upon success. Include a well-labeled diagram to illustrate each step from transaction selection to block propagation.

2. Compare and contrast traditional distributed database systems with blockchain-based distributed ledgers in terms of data storage, consistency models, and trust assumptions. How does the use of consensus algorithms in blockchain replace centralized coordination in distributed databases?

3. A new node joins the Bitcoin network and downloads the latest block headers from its peers. Meanwhile, a miner on the network successfully mines a new block and broadcasts it. However, the new node receives two conflicting blocks referencing the same previous block.

   Based on your understanding of the Bitcoin block structure and peer-to-peer networking, explain how the new node will validate the received blocks and decide which one to add to its local blockchain. Discuss how Merkle roots, proof-of-work, and longest chain rules influence the decision.

4. A startup is designing a new blockchain platform for a supply chain application. The platform must be energy-efficient, provide fast transaction finality, and tolerate up to one-third of malicious or faulty nodes.

   Based on these requirements, which distributed consensus algorithms would you recommend from among Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT)? Justify your choice by comparing how each algorithm meets or fails the startup's needs.

5. An organization wants to implement a blockchain system to manage sensitive data and improve transparency. They are considering whether to adopt a public blockchain or a private blockchain.

   Evaluate the advantages and disadvantages of using a public blockchain versus a private blockchain for this system. Discuss aspects like security, scalability, control, cost, and privacy. Based on your evaluation, which type of blockchain would you recommend and why?

6. A blockchain developer writes a smart contract in Solidity and wants to deploy it on the Ethereum network. Describe the complete process from compiling the Solidity code to deploying the contract on the Ethereum blockchain and finally executing its functions via the Ethereum Virtual Machine (EVM).

   Explain how the EVM handles the execution of smart contracts in a secure and deterministic way across all network nodes.

7. A consortium of banks wants to build a permissioned blockchain network using Hyperledger Fabric to securely share transaction records while maintaining data privacy among participants.

   Explain how Hyperledger Fabric's architecture—including peers, ordering service, channels, chaincode, and Membership Service Provider (MSP)—supports this use case. How do these components work together to ensure transaction privacy, consensus, and secure membership management in the network?

8. Write a Solidity smart contract for a simple decentralized application (DApp) that allows the owner to add items with details such as name and price. Include the following in your contract:

   - Use of different data types (e.g., string, uint256, address, bool)
   - Access modifiers to restrict certain functions only to the owner
   - Events to log the creation of items and purchase actions

   Explain how your contract manages data, restricts access, and emits events.

9.a) How can blockchain technology be utilized to improve the transparency, security, and efficiency of eGovernance systems? Discuss specific use cases such as digital identity management, voting, and public record keeping, highlighting the benefits and challenges.

(OR)

9.b) Discuss how the integration of blockchain technology and artificial intelligence (AI) could shape the future of digital privacy. What are the potential benefits and challenges of using these technologies together to protect user data and enhance trust in digital ecosystems?

10.a) Why is collision resistance a critical property of hash functions in blockchain systems? Explain what could go wrong in a blockchain if the hash function used is not collision-resistant. Provide a real-world or theoretical example to support your explanation.

(OR)

10.b) Explain the process of forming a Merkle tree from a set of blockchain transactions. How is a Merkle root computed, and how can Merkle proofs be used to verify the inclusion of a specific transaction without revealing the entire block? Illustrate with a simple example involving at least five transactions.

⇔⇔⇔ **E/G/TY** ⇔⇔⇔