Nirma University

Institute of Technology

Semester End Examination (IR), December - 2023

B. Tech. in Computer Science and Engineering, Semester-VII

2CSDE93-O Blockchain Technology

Roll / Exam No. | Supervisor's initial with date

Time: 3 Hours | Max. Marks : 100

Instructions:
1. Attempt all questions.
2. Figures to right indicate full marks.
3. Use section-wise separate answer book.
4. Draw neat sketches wherever necessary.

SECTION – I

Q-1. Do as directed: **[18]**

A CO2, BL1	Discuss the process of creating and verifying a digital signature.	**6**
B CO3, BL3	Discuss how Sybil and denial of service (DoS) attacks occur in the Proof of Work-based systems. What are the solutions for resisting these? Give proper and justified examples.	**6**
	OR	
B CO3, BL3	How does Proof of Elapsed Time (PoET) achieve consensus without relying on a computationally expensive process like Proof of Work? What is the role of trusted execution environments (TEEs) in the PoET consensus algorithm?	**6**
C CO2, BL3	Suppose at a given instance, the difficulty set by the BitCoin network is 63, with the last 2016 blocks mined in 10 days. What will be the next computed value of the difficulty [use ceiling to round off to the next integer]?	**6**

Q-2. Do as directed: **[16]**

A CO4, BL5	Show how blockchain can improve the security and privacy of patient data by providing a decentralized and immutable record of medical records, prescriptions, and insurance claims. Explain how it enables real-time access to accurate patient information, facilitates interoperability between healthcare providers, and enhances data sharing for medical research while ensuring patient confidentiality.	**6**
	OR	
A CO4, BL5	Discuss how by leveraging blockchain, educational institutions can streamline administrative processes, enable lifelong learning, facilitate transparent research, and provide a more transparent and verifiable ecosystem for students, educators, and employers.	**6**
B CO4, BL6	Smart contracts can represent and manage ownership of physical or digital assets through tokenization. This includes assets like real estate, artwork, collectibles, and financial instruments. Smart contracts can facilitate fractional ownership, streamline transactions, and enable global access to investment opportunities. Design a smart contract for the same. Identify the individuals, organizations, or systems that will interact with the smart contract. What are the conditions or requirements for the	**10**

smart contract to execute? Determine the criteria that need to be met for the smart contract to perform its intended actions.

Q-3. Do as directed: **[16]**

A CO2, BL3	Suppose we have given 15 transactions (numbered from 1 to 15). Initially, draw the merkle tree from the given set of transactions. Identify its root node value along with its post-order and pre-order traversals. In the merkle tree node value 1 means hash of transaction 1, node value 2 means hash of transaction 2, node value 12 means the combined hash of transactions 1 and 2, and so on).	**8**
B CO2, BL3	In a public-key system using the RSA algorithm, you intercept the cipher-text C = 10 sent to a user whose public key is e = 5 and n = 35. Show the steps to calculate the plaintext M.	**8**

SECTION – II

Q-4. Do as directed: **[18]**

A CO1, BL2	Consider a distributed system with 5 nodes, out of which 2 nodes are faulty and exhibit Byzantine behaviour. The remaining 3 nodes are honest and follow the protocol. Each node has one vote. Will the system be able to reach a consensus in this scenario? Why or why not?	**6**
B CO1, BL4	Explain the concept of fault tolerance in state machine replication and its importance. How does state synchronization occur among the nodes in a state machine-replicated blockchain?	**6**
	OR	
B CO1, BL4	Differentiate between crash fault and byzantine fault.	**6**
C CO1, BL1	What is a consortium blockchain, and how does it differ from other types of blockchains? What are the potential challenges or considerations in establishing a consortium blockchain?	**6**

Q-5. Do as directed: **[16]**

A CO4, BL2	Discuss the need for Hyperledger Fabric framework along with its implementation perspective.	**6**
	OR	
A CO4, BL2	What are decentralized applications (Dapp)? How do they work? What are the benfits of Dapp?	**6**
B CO3, BL4	Which scenario of the three Byzantine Generals' problem put the entire system in dilemma? How to avoid this situation? Give proper justification.	**10**

Q-6. Do as directed: **[16]**

A CO3, BL1	Discuss the working procedure of RAFT consensus algorithm. How it is used to elect a leader? What does RAFT algorithm do upon the current leader's failure in the multiple-leader scenario?	**8**
B CO3, BL4	Consider a scenario of PAXOS consensus algorithm where there are no faulty nodes in the system. How to handle the failure of acceptor nodes in both prepare and accept phases. Explain it by taking a suitable example with a diagram.	**8**

****