Nirma University

Institute of Technology

Semester End Examination (IR), December 2022

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

2CSDE93: 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 **CO1, BL1** Differentiate between distributed and decentralized systems. Whether blockchain is one of them or not? Justify your answer by taking any relevant example. **6**

B **CO1, BL2** PoW has been criticized for its high and continually rising mining cost. Discuss how mining cost impacts the tamper resistance attribute of public blockchains. **6**

OR

B **CO1, BL2** How does Proof of Elapsed Time (PoET) justify the equal probability of every node in blockchain to get a chance to mine the block? Explain in detail. **6**

C **CO1, BL3** Say, three independent miners propose the following three blocks (containing the transactions enclosed in [ ]) **6**

B1=[T09, T12, T13, T14, T16],
B2=[T10, T11, T13, T15, T16], and
B3=[].
[ ] represents empty block of transaction.

Consider that the consensus algorithm is PoW. Once the network achieves consensus, which of the following blocks is likely to get added to the main chain, given the blockchain has a fork at the end with transactions {T10, T11, T15} and {T09, T12, T14}? Justify your answer.

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

A **CO4, BL5** India is a democratic country, where people elect government ministers using an electoral system that is managed by the Election Commission of India. However, recently, we have seen several issues with the Indian electoral system, which raises the integrity question for the user vote. Discuss how the blockchain-based decentralized network resolves the problems of vote integrity. **6**

OR

A **CO4, BL5** Goods and service tax (GST) is an indirect tax covering various goods and services during the production and service stages. The process of GST involves multiple parties and all have to pay their taxes **6**

	individually to the government. Show how the blockchain-based decentralized network handles GST-based transactions.	
B **CO4, BL6**	Design a smart contract for test voting mechanism using the *Ethereum* blockchain. Assume three contestants for which the public would vote. Display the count of votes for each contestant. If a user has voted for a particular contestant, then revoting is not allowed. Use diagrams to justify the interaction between various entities.	**10**

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

A **CO2, BL3**	Explain what a Merkle tree is and for what purpose(s) it is used in the Bitcoin blockchain. In particular, explain how the use of a Merkle tree in a Bitcoin block is superior to simply putting all transactions directly inside the block header. Suppose you have eight data points — 8 to 1. Represent the post-order traversal of the Merkle Tree. (Note: Here, 8 means hash of 8, 43 means the combined hash of 4 and 3, and so on.	**8**
B **CO2, BL3**	Explain the working of PoW with proper illustration. Suppose at a given instance, the difficulty set by the BitCoin network is 55, with the last 2016 blocks mined in 11 days. What will be the next computed value of the difficulty [use ceiling to round off the value]?	**8**

SECTION – II

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

A **CO1, BL2**	In practical byzantine fault tolerance (PBFT), why do you require $3f+1$ replicas to ensure safety in an asynchronous system where there are f faulty nodes? Explain with the help of an example.	**6**
B **CO1, BL2**	Suppose, you develop a system using RAFT consensus protocol. Using this consensus mechanism, your system identifies that the leader is Byzantine. What will the system do now? Justify your answer.	**6**
	OR	
B **CO1, BL2**	Discuss in detail how state machine replication is helpful in distributed consensus.	**6**
C **CO1, BL1**	Differentiate between public, private, and consortium blockchains taking at least 2 examples of each.	**6**

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

A **CO3, BL2**	What will be the problems caused if the executions in a smart-contract platform become non-deterministic?	**6**
	OR	
A **CO3, BL2**	If always the highest number proposal will be selected in PAXOS, then the faulty or compromised node can easily get the proposal by sending a random biggest number. How does the network make sure to counter such an attack?	**6**
B **CO3, BL4**	Alice wants to develop a secure distributed system where she wants to keep track of the node identity. Additionally, she wants fixed message content representation although any node in the system can transfer the message of any size. You as a system consultant, suggest a consensus protocol to Alice, which is extremely suitable for her system. Explain the consensus protocol in detail.	**10**

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

A **CO2, BL1**	Discuss the failure of leader and follower in RAFT consensus and how consensus is achieved in such a scenario.	**8**
B **CO2, BL3**	Suppose there are 5 (with ids 1 to 5) nodes in a distributed system. While in process of reaching consensus, node 1 suggests a proposal with a proposal number 405. In the same way, node 4 suggests a proposal with a proposal number 411. Now, the node 1 being a malicious node immediately proposes another proposal with a proposal number 415. Considering PAXOS as the underlying consensus algorithm, how the system will reach consensus in this scenario? Explain in detail how PAXOS consensus works in this defined scenario.	**8**