Nirma University

Institute of Technology

Sessional Examination, October 2023
B. Tech CSE, Semester: VII
2CSDE93: Blockchain Technology

Roll/ Exam No		Supervisor's initial with date	

Time: 02 Hour   Max Marks: 50

Instructions:

i) Attempt all questions.
ii) Figures to the right indicate full marks.
iii) Draw neat sketches wherever necessary.
iv) Assume necessary data wherever required and specify clearly.

Q.1. Consider a scenario of one faulty commander and two non-faulty lieutenants in the three Byzantine Generals problem. A faulty commander sends two different messages to lieutenants (attack to Lieutenant 1 and retreat to Lieutenant 2). Which command the lieutenants will follow and why? Show diagrammatic low of message in the defined scenario. CO3, BL3 **[08]**

Q.2. Explain the concept of public key cryptography. How digital signature supports public key cryptography. Explain with proper illustration and diagrammatic representation. CO2, BL1 **[08]**

Q.3. Smart contracts can be used to automate and streamline supply chain processes, including tracking and verifying the movement of goods, ensuring compliance with regulations, and facilitating transparent and efficient transactions between suppliers, manufacturers, distributors, and retailers. 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 smart contract to execute? Determine the criteria that need to be met for the smart contract to perform its intended actions. CO4, BL4 **[08]**

Q.4. 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. CO2, BL4 **[08]**

Q.5. Discuss the working procedure of RAFT Consensus algorithm. How is it used to elect a leader? What RAFT CO1, BL2 **[08]** algorithm do upon the failure of current leader in the multiple leader scenario?

Q.6. Suppose, you have developed an asynchronous system that can tolerate at most f faulty nodes. What is the minimum number of the similar responses needed for concluding the decision? How many minimum number of nodes are required for the same? Justify your answer. CO3, BL3 **[05]**

Q.7. Suppose at a given instance, the difficulty set by the Bitcoin network is 75, 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]. CO1, BL5 **[05]**

-------------------------End---------------------------