Nirma University

Institute of Technology

Semester End Examination (IR), December 2021

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

2CSDE93: Blockchain Technology

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

Time: 2 Hours Max. Marks: 50

Instructions:
1. Attempt all questions.
2. Figures to right indicate full marks.
3. Draw neat sketches wherever necessary.
4. Attempt questions in sequence only.

Q-1.	**Do as directed:**	
A CO1BL4	Why the Hyperledger is called as a modular blockchain technology? What are the differences between Hyperledger and Ethereum?	**[15]** [05]
B CO1BL2	What if Alice wants to send two same transactions intentionally? I mean X to Y 30 BTC, she wants to send twice. How will the other peers get to know that this is not a redundant transaction?	[05]
	OR	
B CO4BL2	List out the advantages of Blockchain-enabled Cheque Clearance System for financial institutions. Use diagrammatic approach to validate your answer.	[05]
C CO2BL3	Describe the usage of smart contracts for supply chain management. Also, illustrate how the smart contract can be framed between retailer, customer, and manufacturer.	[05]
Q-2.	**Do as directed:**	
A CO2BL2	Alice wants to develop a secure distributed system where she wants to keep track of the node identity. Additionally, she wants to use a fixed message content representation scheme in which 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.	**[20]** [10]
	OR	
A CO2BL4	Suppose, 15 trustworthy nodes are performing some task distributely. As per the process, at a certain interval, every node of the team shares the results for making the consensus. After starting the task, 7 trustworthy nodes drop the plan and they are replaced by 7 other nodes whose trustworthy information is unknown. After joining the new nodes, some discrepancy occurs in the system, although all the nodes are running correctly without any software or hardware error. What is the type of fault it is in the context of distributed consensus? Give proper reason for your answer.	[10]
B CO4BL4	After 21 million bitcoins are mined, will not the use of bitcoins come to an end? (i) The hardware during that time will be many times more fast,	[10]

complex and expensive. How will miners survive without rewards? The miners will thus cease to express interest as they will run into heavy losses. This will bring mining to a halt and eventually no one will be there to generate new blocks.
(ii) Can this prove out to be tragic for all those who will be investing into bitcoin? Because their cryptocurrency will be jammed into that network from where they can't move it anywhere!

Q-3.	**Do as directed:**	**[15]**
A **CO3BL2**	PoB works by burning PoW mined blocks". Does it mean that PoB does not exist on its own, I mean it is to be implemented along with PoW to control the power and Monopoly problem that may arise from PoW.	[05]
B **CO3BL2**	Describe message integrity and how hash functions are used for checking the message integrity? Discuss all possible criteria.	[05]
C **CO2BL1**	Write your view point on the "Design Limitations of Permissioned environment". Do we really need to execute contracts at each node in the Permissioned Blockchain?	[05]