Reg. No.: 20BCE1707

Name :

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act 1956)

Continuous Assessment Test CAT – I – SEP 2023

Programme	:	B.Tech Specialization in Computer Science (Core)	Semester	:	Fall 2023-2024
Course Title	:	Blockchain and Cryptocurrency Technologies	Code	:	CSE1006
			Class Nbr(s)	:	CH2023240100191 CH2023240100189
Faculty(s)	:	Dr. Prasad M & Dr. Prabhakaran R	Slot	:	E2
Time	:	1 ½ Hour	Max. Marks	:	50

Answer All questions

Q.No.	Sub. Sec.	Question Description	Marks
1.		A transaction was done for 100 BTC from X to Y. Based on the above transaction, a Hyrid model was implemented for user authentication and message authentication. Illustrate and verify the transactions based on the decentralized system's perspective?	10
2.		Contemplate transaction from 1 to 8, build a Merkle tree for the same with the which need to express the hashes with phases of implementation in Blockchain.	10
3.		Let's assume a transaction of 100ETH was done between Alice and bob. Transaction is available for miners(nodes) for verification. At that point of instance X creates a copy of the transaction and sends it to Y. X uses a higher computing device to control the transaction and makes it available to Y. In this scenario bob didn't receive the transaction amount. Consider this scenario and provide the visual representation of blocks with hash function properties.	10
4.		Let's assume a transaction of 100ETH was done between Alice and bob. Transaction is available for miners(nodes) for verification. At that point of instance X creates a copy of the transaction and sends it to Y. X uses a higher computing device to control the transaction and makes it available to Y. In this scenario bob didn't receive the transaction amount. Consider the above scenario and describe the design and working of Hash algorithm.	10
5.		Consider a transaction was done, illustrate the transaction based on consensus algorithm.	10

VIT
Vellore Institute of Technology

Reg. No. : 20BCE1707

Final Assessment Test (FAT) - November/December 2023

Programme	**B.Tech.**	Semester	**FALL SEMESTER 2023 - 24**
Course Title	**BLOCKCHAIN AND CRYPTOCURRENCY TECHNOLOGIES**	Course Code	**CSE1006**
Faculty Name	**Prof. Prabakaran R**	Slot	**E2+TE2**
		Class Nbr	**CH2023240100189**
Time	**3 Hours**	Max. Marks	**100**

Section 1 (10 X 10 Marks)
Answer all questions

01. Create a transaction of 100 BTC from X to Y. Based on the above said transaction you have to devise a Hybrid model to implement the user authentication and message authentication, so that the Y can verify the transactions genuinely using the Hybrid model. **[10]**

02. A). Contemplate transaction from 1, 2 4, 8, 9, 3, 5 build a Merkle tree for the same with the which need to express the hashes with a diagram. [5 Marks] **[10]**
B). In the above said Merkle tree a transaction is duplicated by an intruder. Illustrate with a diagram how the changes by the intruder will be identified. [5 Marks]

03. *Let's assume a transaction* of 1000ETH was done between Alice and bob. Transaction is *available for miners(nodes)* for verification. At that point of instance X creates a copy of the *transaction* and sends *it* to Y. X uses a higher computing device to control the transaction and makes it available to Y. In this scenario bob didn't receive the transaction amount. Consider this scenario and identify the attack and illustrate a solution for it. **[10]**

04. Imagine you are hosting a workshop on the technical aspects of Bitcoin for an audience of software developers interested in blockchain technology. Explain Bitcoin Scripts, the scripting language used in Bitcoin transactions. Describe how Bitcoin Scripts work, including their role in creating custom transaction conditions. Illustrate with real-world examples how Bitcoin Scripts can be used for various purposes, such as multi-signature wallets or time-locked transactions and discuss their significance in enhancing Bitcoin's functionality and security. **[10]**

05. Assume that X wants to send 1000 BTC to Y, and he decides to make this transaction. As an expert in Bitcoin, illustrate in detail the process of this transaction, considering the involvement of mining pools, mining incentives, and potential strategies employed by miners to ensure its successful processing. Discuss the role of mining pools in confirming and adding transactions to the blockchain, the incentives motivating miners to include X's transaction, and any strategic considerations that miners might take into account when selecting which transactions to include in the blocks they mine. And also illustrate the possible attacks. **[10]**

06. Consider you are transferring 100 BTC to a person X. Illustrate how the anonymity is established for the transaction and how de-anonymize will be performed for the same. **[10]**

07. Assume that X wants to send 1000 BTC to Y, and he decides to make this transaction. As an expert in Bitcoin, Illustrate in detail the process of this transaction, considering the involvement of Mixing and decentralized mixing to ensure its successful processing. Discuss the role of mixing in the transaction. [10]

08. Consider you are leading a seminar for a group of technology enthusiasts eager to understand the intricacies of Bitcoin and Altcoin. Describe, step by step, the process by which how they differ and in transaction and algorithms. Discuss how the algorithm efforts to contribute the overall functioning and trustworthiness of the cryptocurrency. [10]

09. Assume that you are participating in a panel discussion on the future of cryptocurrencies at a blockchain technology conference. Elaborate to the audience the key limitations of the current Bitcoin protocol. Subsequently, discuss Ethereum with Bitcoin and the how the smart contracts will be established. [10]

10. You are providing bitcoins for platform service, in this consideration how will you provide secure multi party lotteries based on Bitcoin. Illustrate the security provided by the lottery agency and the platform. [10]