Reg. No.:

Name :

VIT®

Vellore Institute of Technology

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

Re-Continuous Assessment Test CAT – I – October 2023

Programme	: **B.Tech Specialization in Computer Science (Core)**	Semester	:	**Fall 2023-2024**
Course Title	: **Blockchain and Cryptocurrency Technologies**	Code	:	**CSE1006**
		Class Nbr(s)	:	**CH2023240100188**
Faculty(s)	: **Dr. Prabhakaran R**	Slot	:	**E1+TE1**
Time	: **1 ½ Hour**	Max. Marks	:	**50**

Answer All questions

Q.No.	Sub. Sec.	Question Description	Marks
1.		Imagine you're employed as a system engineer at ABC Software Development, where your team is currently engaged in a project for "HFCC BANK." The bank's clientele has requested an enhancement in the security of their financial data, along with the elimination of central authority in their banking operations. Propose a contemporary technology that can meet the customer's requirements. Enumerate the essential elements and procedures that compose the framework of this suggested technology and elucidate their roles in reinforcing security and decentralization.	10
2.		Imagine you are designing a blockchain-based system for a supply chain management company. Each transaction in the supply chain is recorded on the blockchain, and you decide to use Merkle trees to secure the data. In this supply chain blockchain system, explain how the use of Merkle trees can enhance the security and efficiency of verifying the integrity of transactions. Provide an example of how a Merkle tree would be constructed for a specific set of transactions within the supply chain and describe how it facilitates the verification process.	10
3.		You are a security consultant for a company that uses blockchain technology to manage its financial transactions and supply chain information. Recently, the company experienced a significant disruption due to a denial of service (DoS) attack on their blockchain network. Describe the potential impact of a denial of service (DoS) attack on a blockchain network used for financial and supply chain management. Discuss the key vulnerabilities that attackers may exploit in a blockchain system to execute such an attack. Furthermore, propose and explain at least two strategies or security measures that the company could implement to mitigate the risk of future DoS attacks on their blockchain network.	10
4.		Suppose there was a transaction where Alice sent 100ETH to Bob. This transaction was open for verification by miners (nodes) at a specific moment. At that moment, Node X duplicated the transaction and forwarded it to Node Y. Node X, equipped with a more powerful computing device, manipulated and shared the transaction with Node Y. In this situation, Bob did not receive the expected transaction amount. Using the provided scenario, create an explanatory diagram that demonstrates the DoS attack that transpired.	10
5.		You are the Chief Information Officer (CIO) of a blockchain-based financial services company that specializes in digital asset management. Your company has implemented a security strategy involving both hot and cold storage solutions for the safekeeping of digital assets. Describe the advantages and use cases of hot and cold storage in a blockchain-based	10

financial services company. Provide specific examples of situations where each storage method is best suited and explain how these strategies help ensure the security and accessibility of digital assets for your company's clients.