U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

June 2025 Semester End Main Examinations

Programme: B.E. **Semester: VI**
Branch: Computer Science and Engineering **Duration: 3 hrs.**
Course Code: 22CS6PCBLC **Max Marks: 100**
Course: Blockchain

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

B.M.S.C.E. - EVEN SEM 2024-25

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT – I	***CO***	***PO***	**Marks**
1	a)	Differentiate between centralized and decentralized systems with necessary diagrams.	***CO2***	***PO2***	**6**
	b)	Axis Bank Ltd. uses a blockchain network for performing transactions and storing data. Customers feel that it is a good idea to use a blockchain. Identify the various advantages that Axis Bank has by using this approach.	***CO2***	***PO2***	**8**
	c)	Peter and Vincent are two friends who plan to visit a restaurant for dinner on friendship day. The restaurant's door can be opened by using a special code, known only to Peter. What type of protocol is used by Vincent to check if Peter really knows the special code? Illustrate the different phases used in this protocol.	***CO2***	***PO2***	**6**
		OR			
2	a)	Differentiate between zk-SNARK and zk-STARK zero knowledge schemes.	***CO2***	***PO2***	**6**
	b)	Kidwai Research Centre stores critical data of patients having oncology problems on a blockchain. The policy of the research centre is not to share the data to unauthorized persons yet to keep the data transparent to the authorized officials only. Analyze the limitations of this system and justify the same.	***CO2***	***PO2***	**6**
	c)	Identify the type of signature used in the following scenarios and explain the same with required diagrams. i. A message needs to be signed by multiple signers. But the system has limited space for storing keys. Also, the signatures cannot be done asynchronously. ii. A message can be signed by any one member from a trusted group and the identity of the signer must remain unknown. iii. A message needs to be signed by multiple signers and the message can be signed and verified asynchronously.	***CO2***	***PO2***	**8**

			UNIT-II			
	3	a)	Consider the transactions Ta, Tb, Tc, Td, Te, Tf, Tg and Th. Show the construction of Merkel Tree for the above transactions. Also, discuss the importance of Merkel Trees in Blockchain.	***CO1***	***PO1***	**6**
		b)	IBM has decided to use a new consensus algorithm that can provide crash fault tolerance and works in an asynchronous message passing system. Identify the most suitable consensus algorithm and explain its working with suitable diagram.	***CO2***	***PO2***	**8**
		c)	Bitcoin is the most used crypto-currency across the globe today. However, sending or receiving Bitcoins is not a one step process. Illustrate the different stages that a Bitcoin transaction goes through from the time it is initiated on the network.	***CO1***	***PO1***	**6**
			OR			
	4	a)	Proof of Work is a solution to the Byzantine Generals Problem. Justify this statement and explain the working of the algorithm.	***CO2***	***PO2***	**6**
		b)	Intel Corporation uses a Blockchain network for performing all its data transactions. Intel now wants a new Consensus algorithm that could terminate without any additional communication costs. Identify the most suitable consensus algorithm and explain its working with suitable diagram.	***CO2***	***PO2***	**8**
		c)	Discuss the characteristics of genesis block and orphan blocks in Bitcoin network with suitable diagrams.	***CO1***	***PO1***	**6**
			UNIT-III			
	5	a)	John is travelling to India by air and has bought insurance for his flight. Unfortunately, the flight gets cancelled and the airlines does not make any alternative arrangements for his travel nor do they give a refund. Analyze how smart contracts in blockchain could solve this problem. Also, enlist and explain the properties of smart contacts.	***CO2***	***PO2***	**8**
		b)	Illustrate the working of an Ethereum Virtual Machine with a neat diagram.	***CO1***	***PO1***	**6**
		c)	Write a smart contract that demonstrates the use of the following: i) Inheritance ii) View functions	***CO2***	***PO2***	**6**
			OR			
	6	a)	A multinational corporation aims to improve supply chain transparency by deploying smart contracts on Ethereum to track the journey of goods from production to delivery. Outline the steps involved in deploying a series of interconnected smart contracts for supply chain traceability. Analyze how blockchain technology enhances transparency and accountability in supply chain management.	***CO2***	***PO2***	**10**
		b)	Develop a smart contract to illustrate the following: Sending money to an authorized account and receiving money from an authorized account. Also display the sender and receiver address.	***CO2***	***PO2***	**10**

B.M.S.C.E. - EVEN SEM 2024-25

			UNIT – IV			
	7	a)	The addresses generated in Bitcoin are highly secure and undergo various stages during their creation. Illustrate the different steps involved in the Bitcoin address generation with a neat diagram.	***CO1***	***PO1***	**8**
		b)	Compare and contrast among the following Bitcoin wallets: i) Non-determinitic wallets ii) Deterministic wallets iii) Heirarchical Deterministic wallets.	***CO2***	***PO2***	**6**
		c)	Analyze the drawbacks of using Proof of Work for consensus. Identify and explain any two alternatives for PoW.	***CO2***	***PO2***	**6**
			OR			
	8	a)	Explain the following: i) Double Spending ii) Sybil Attack	***CO1***	***PO1***	**6**
		b)	Consider a scenario and explain the process of sending payment using the Blockchain wallet for mobile devices.	***CO2***	***PO2***	**8**
		c)	Outline some of the alternatives to PoW.	***CO1***	***PO1***	**6**
			UNIT – V			
	9	a)	Illustrate the different components of a Hyperledger architecture with a neat diagram.	***CO1***	***PO1***	**8**
		b)	Identify and explain the different components of the Hyperledger Fabric required for transaction execution.	***CO1***	***PO1***	**6**
		c)	Analyze the need for using transaction families. Explain how this is accomplished in Sawtooth network.	***CO2***	***PO2***	**6**
			OR			
	10	a)	List out the features and benefits of the Hyperledger Sawtooth	***CO1***	***PO1***	**10**
		b)	Design a transaction family for a voting system application using Hyperledger Sawtooth. Include necessary components such as transaction processors, state variables, and transaction validation logic. Justify your design choices.	***CO3***	***PO3***	**10**

B.M.S.C.E. – EVEN SEM 2024-25

******