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

Autonomous Institute Affiliated to VTU

June 2025 Semester End Main Examinations

Programme: B.E.   **Semester: VI**
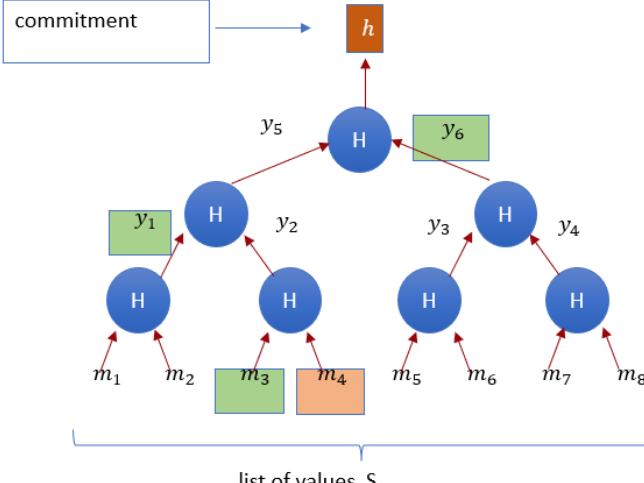
Branch: Computer Science and Engineering   **Duration: 3 hrs.**

Course Code: 23CS6PEBLC   **Max Marks: 100**

Course: Blockchain Technology

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

<table>
<tr><td colspan="3" align="center">UNIT - I</td><td>CO</td><td>PO</td><td>Marks</td></tr>
<tr><td rowspan="3">1</td><td>a)</td><td>Describe how blocks are generated in a Blockchain and explain the relationship between transactions and blocks.</td><td>CO1</td><td>PO1</td><td>7</td></tr>
<tr><td>b)</td><td>Indian Bank is currently using a distributed network for core banking. The customers are facing the following problems.
• The amount being transferred is sometimes prone to eavesdropping attacks
• Agricultural loan is not transparently distributed to the farmers.
Identify a solution to handle the problems and justify your solution with the various characteristics.</td><td>CO1</td><td>PO1</td><td>8</td></tr>
<tr><td>c)</td><td>Define Merkle tree. Bob is verifying an inclusion proof for m4 in the Merkle tree. If the proof provided is $\pi = (m_3, y_1, y_6)$ what steps must Bob follow to verify the proof?

</td><td>CO1</td><td>PO1</td><td>5</td></tr>
<tr><td colspan="3" align="center">OR</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>a)</td><td>Describe how the generic elements of blockchain work together to enable the fundamental functioning of any blockchain system.</td><td>CO2</td><td>PO2</td><td>7</td></tr>
</table>

		b)	Explain how ECDSA works in blockchain platforms to validate messages and provide data integrity services.	*CO2*	*PO2*	**7**
		c)	Illustrate with a suitable diagram how a distributed hash table works.	*CO2*	*PO2*	**6**
			UNIT - II			
	3	a)	Explain the three phases of PBFT protocol and discuss its strengths and weaknesses.	*CO1*	*PO1*	**7**
		b)	Describe the complete lifecycle of a Bitcoin transaction and explain how miners select transactions, and the impact of transaction fees on confirmation time.	*CO1*	*PO1*	**7**
		c)	What are the various types of Bitcoin wallets used for storing private keys, and how does each wallet facilitate transactions on the Bitcoin network?	*CO1*	*PO1*	**6**
			OR			
	4	a)	What are the key roles and tasks performed by a Bitcoin miner once a node connects to the Bitcoin network? Discuss the steps involved in the mining algorithm.	*CO1*	*PO1*	**8**
		b)	Identify the most suitable consensus mechanism for a global cryptocurrency intended for financial transactions. Justify your answer with a comparison of PoW, PoS, and DPoS across relevant parameters.	*CO1*	*PO1*	**7**
		c)	Discuss briefly various Bitcoin payment techniques.	*CO1*	*PO1*	**5**
			UNIT - III			
	5	a)	Draw an overall Ethereum ecosystem architecture and briefly explain its elements.	*CO1*	*PO1*	**8**
		b)	Consider the given scenario: You are tasked with developing a smart contract for a basic Ethereum wallet. The wallet should: • Accept Ether deposits from any address. • Only allow the contract owner to withdraw funds. • Log any unexpected direct Ether transfers using the fallback function. Write a Solidity contract snippet that satisfies the above requirements.	*CO1*	*PO1*	**7**
		c)	Describe the steps involved in transferring funds between two Ethereum clients.	*CO1*	*PO1*	**5**
			OR			

				CO1	PO1	8

6	a)	Explain the following:
		   i. EVM execution environment
		   ii. Machine state of EVM
		   iii. Iterator function of EVM
				CO1	PO1	8

	b)	Consider the given scenario: You are designing a smart contract for a donation system. The contract should: • Allow anyone to send Ether as a donation. • Allow only the contract owner to withdraw the funds. • Use a modifier to restrict access to the withdraw function. • Use a fallback function to log any unexpected transactions. Write a Solidity contract that implements these features.		CO1	PO1	7
	c)	Explain the concept of reentrancy attacks and arithmetic overflows/underflows in smart contracts. How can these issues be exploited, and what measures can be taken to prevent them?		CO1	PO1	5
		UNIT - IV				
7	a)	Illustrate the popular blockchain platforms for DApp development.		CO1	PO1	8
	b)	Explain the key characteristics of a DApp for a real time project.		CO1	PO1	6
	c)	Discuss the various advantages and disadvantages of using DApps for developing a healthcare system.		CO2	PO2	6
		OR				
8	a)	Illustrate the salient features of DApps. Also, discuss how a DApp differs from traditional applications.		CO1	PO1	10
	b)	Developing a distributed application is not similar to any web application development. Analyze the different components of DApp development that a developer needs to consider for building a successful DApp.		CO1	PO1	10
		UNIT - V				
9	a)	Explain the design principles of Hyperledger in detail.		CO1	PO1	7
	b)	Describe the core components of Hyperledger Sawtooth and explain how these components interact with each other to support blockchain operations.		CO1	PO1	7
	c)	Explain the process of tokenization.		CO1	PO1	6
		OR				
10	a)	Explain the transaction lifecycle in Hyperledger Fabric with a neat diagram.		CO1	PO1	7
	b)	Explain the blockchain services provided at the core of Hyperledger Fabric.		CO1	PO1	7
	c)	Describe the different types of token offering mechanisms.		CO1	PO1	6

******