Q. Code: 598325

Reg. No. | | | | | | | | | | | | | |

M.E/ M. TECH.DEGREE EXAMINATIONS, MAY 2024

Second Semester

CF22203 – BLOCKCHAIN FOR SECURITY

(*Cyber Forensics and Information Security*)

(Regulation 2022)

TIME:3 HOURS **MAX. MARKS: 100**

COURSE OUTCOMES	STATEMENT	RBT LEVEL
CO 1	Elucidate the requirements of a blockchain.	**5**
CO 2	Design a simple blockchain based application.	**4**
CO 3	Implement Consensus mechanism in blockchain.	**4**
CO 4	Deploy sample applications over Hyperledger.	**4**
CO 5	Explain the requirement of mining in blockchain.	**4**

PART- A(20x2=40Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	Point out the principles act as backbone for blockchain technology.	**1**	**4**
2.	Demonstrate the features of hash function.	**1**	**3**
3.	List the applications of distributed hash table.	**1**	**3**
4.	Summarize the properties of digital signature.	**1**	**2**
5.	Compare hash pointer and Merkle root in blockchain.	**2**	**4**
6.	Sketch the layered architecture of blockchain technology.	**2**	**3**
7.	Identify the attributes of block in blockchain system.	**2**	**2**
8.	Differentiate between a distributed system and a decentralized system.	**2**	**2**
9.	Describe distributed consensus.	**3**	**2**
10.	Discuss the requirement that must be met in order to produce the desired results in a consensus algorithm.	**3**	**3**
11.	Interpret eventual consistency in blockchain technology in your own words.	**3**	**3**
12.	Indicate the types of proof of stake consensus algorithm.	**3**	**3**
13.	List the categories of projects under Hyperledger.	**4**	**2**
14.	Differentiate between Chaincode and smart contract in Hyperledger Fabric.	**4**	**2**
15.	Explain how Hyperledger sawtooth prevents DAO hacks and mitigate Denial of service.	**4**	**4**
16.	List the type of messages passed between nodes in Fabric.	**4**	**2**
17.	Compare and contrast the two types of nodes in Bitcoin network.	**5**	**3**
18.	Summarize the techniques and tools used to enhance the security of smart contract.	**5**	**2**

			Marks	CO	RBT LEVEL
19.		Identify the types of wallets used in bitcoin.	**5**	**2**	
20.		Demonstrate how a blockchain based IoT model differs from traditional IoT network paradigm.	**5**	**3**	

PART- B (5x 10=50Marks)

			Marks	CO	RBT LEVEL
21. (a)	**(i)**	Outline the properties that make the hash function as an effective cryptographic tool.	**(5)**	**1**	**4**
	(ii)	Illustrate in detail about how blind signatures ensure privacy and unlinkability in transactions.	**(5)**	**1**	**4**
		(OR)			
(b)		Break down the steps involved in the Elliptic Curve Digital Signature Algorithm (ECDSA). Also mention the advantages of ECDSA.	**(10)**	**1**	**4**
22. (a)		An ABC firm set up the distributed environment for the project and they are on the verge of completing their project. The firm wanted to use the set up to create decentralized storage network using blockchain as like filecoin. Evaluate requirements of decentralization in the context of blockchain for creating decentralized storage network.	**(10)**	**2**	**4**
		(OR)			
(b)		Consider Mr. Kumar is a consultant advising a multinational corporation interested in implementing blockchain technology for its supply chain management. The corporation operates in multiple countries and deals with a diverse range of suppliers and distributors. They want to explore different types of blockchain networks and choose the most suitable one for their needs. Explain the different types of blockchain networks and working principles to the corporation's management team, and point out the suitable blockchain network for their supply chain management solution?	**(10)**	**2**	**4**
23. (a)		Imagine Ms. X is a blockchain consultant advising a startup company interested in launching a new cryptocurrency. The company's team is curious about the various consensus algorithms used in blockchain networks and how they differ. Categorize and explain the different consensus algorithms to the team, and recommend one consensus algorithm for their cryptocurrency project?	**(10)**	**3**	**4**

(OR)

(b)	**(i)**	Illustrate briefly how the Proof of Work (PoW) consensus algorithm operates within blockchain networks.	**(5)**	**3**	**4**
	(ii)	Explain briefly the phases in Practical Byzantine Fault Tolerance (PBFT) used to achieve consensus.	**(5)**	**3**	**4**
24. (a)		Consider a healthcare consortium that aims to create a secure and interoperable electronic health record (EHR) system using Hyperledger Fabric. Explain the components of Hyperledger Fabric for EHR system and chaincode implementation to ensure the privacy, data integrity, and access control of patient health records across multiple healthcare providers.	**(10)**	**4**	**4**

(OR)

(b)		Imagine a team tasked with developing a supply chain tracking application for a multinational corporation using Hyperledger Sawtooth. Explain in detail about the consensus mechanism and transaction flow within the network to ensure the integrity, transparency, and efficiency of the supply chain tracking process.	**(10)**	**4**	**4**
25. (a)		Construct the blind auction smart contract using solidity.	**(10)**	**5**	**3**

(OR)

(b)	**(i)**	Illustrate in detail about how blockchain can be used in financial applications.	**(5)**	**5**	**3**
	(ii)	Explain in detail about how blockchain can be used in government applications.	**(5)**	**5**	**3**

PART- C (1x 10=10Marks)

(Q.No.26 is compulsory)

		Marks	CO	RBT LEVEL
26.	Mr. Rakesh is working in xyz organization which involves in a project to collect public confidential information for government schemes. The information has to be sent through an overlay network to maintain the data in decentralized application. Recommend the suitable secure hash algorithm and Evaluate the steps involved in message digest generation using the algorithm.	**(10)**	**1**	**5**

****