Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S8 (R,S) Exam April 2025 (2019 Scheme)

Course Code: CST428

Course Name: BLOCKCHAIN TECHNOLOGIES

Max. Marks: 100 **Duration: 3 Hours**

PART A

Answer All questions, each carries 3 marks. Marks

1		Mention the properties and applications of digital signatures.	(3)
2		Distinguish between symmetric and asymmetric cryptography.	(3)
3		What is the significance of Genesis block in the blockchain?	(3)
4		What are Merkle trees? How can Merkle tree increase the security of blockchain?	(3)
5		What is a wallet? Explain its types.	(3)
6		Explain how the RAFT consensus algorithm operates to achieve agreement among peers in a blockchain.	(3)
7		Define smart contracts and mention its relevant properties	(3)
8		Enumerate benefits and limitations of using blockchain technology.	(3)
9		Illustrate the concept of inheritance in Solidity language.	(3)
10		Explain the role of the Ethereum Virtual Machine in the Ethereum network.	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11	a)	Perform encryption and decryption using RSA Public Key cryptographic technique for p=7; q=11, e=13; M=5. Illustrate the public key and private key generation.	(7)
	b)	Depict the working of Advanced Encryption Standard (AES) with a neat diagram explaining each round of operations.	(7)

OR

12	a)	Explain the working of Elliptic Curve Cryptography algorithm.	(7)
	b)	Explain the design of SHA-256 and its compression function deployed in blockchain.	(7)

Module II

13	a)	Explain the generic elements of blockchain. Illustrate the working of Block chain with a neat diagram.	(7)
	b)	Compare the consensus mechanisms: Proof of Work, Proof of Stake and Delegated Proof of Stake.	(7)

A5

OR

14 a) Compare and contrast the various types of Block chain and their relevance in the real world use cases. (7)

b) Explain the ecosystem of decentralisation and its methods with respect to blockchain. (7)

Module III

15 a) Explain how Paxos protocol can be used to achieve consensus in crash fault tolerance. (7)

b) Describe the various fields that make up a transaction in Bitcoin. Explain how a payment is sent using a Bitcoin network in terms of user's perspective. (7)

OR

16 a) Show how Practical Byzantine Fault Tolerance can achieve consensus in the presence of Byzantine faults. (7)

b) What is the role of a Bitcoin miner? Explain the mining process used in Bitcoin with the help of a diagram. (7)

Module IV

17 a) Explain the aspects and working of Decentralized Applications (DApps). (7)

b) Illustrate with a use case, the application of blockchain technology in government Sector (7)

OR

18 a) Discuss the legal and ethical implications of blockchain technology. (7)

b) Explain the generic data flow of Oracle in smart contracts. Describe any three types of Oracles used in blockchain to interact with the external world. (7)

Module V

19 a) What are the various control structures available in Solidity language. (7)

b) Write a Solidity smart contract for a simple voting system. (7)

OR

20 a) Compare Bitcoin and Ethereum. Explain the various elements present in the Ethereum blockchain. (7)

b) Describe how transactions are processed in Ethereum. Explain the concept of gas and its impact on transaction processing. (7)

****