Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S8 (S) Examination September 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 What is the significance of "Merkle root" stored in the block header? (3)

2 List out the desirable properties for a cryptographic hash function. (3)

3 Depict the generic structure of a block in blockchain. (3)

4 Describe how full ecosystem decentralization is possible in blockchain. (3)

5 Explain the terms Genesis block and coinbase transaction. (3)

6 What is "hash rate" in Bitcoin? How does it vary with respect to time? (3)

7 What is a Decentralized Autonomous Organization (DAO)? (3)

8 Give any two use cases where blockchain and AI can be combined. (3)

9 Distinguish between 'mainnet', 'testnet' and 'privatenet' in Ethereum blockchain. (3)

10 Jordan has to pay Taylor 1 ETH. An ETH transfer requires 21,000 units of gas. The base fee is 10 gwei and Jordan also includes a tip of 2 gwei. What will be the gas fee for this transaction? How much ETH will be deducted from Jordan's account? (3)

PART B

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

Module I

11 a) Explain the RSA key generation algorithm. Also show how RSA generates public and private keys from the values P = 17 and Q = 11. (7)

b) Illustrate the digital signature generation and verification process. (7)

OR

12 a) Explain with a neat block diagram, the steps involved in AES algorithm. (7)

b) Demonstrate the design of SHA-256 cryptographic hash function and its applications. (7)

Module II

13 a) Explain different types of blockchain based on technical and business usage perspective. (7)

b) Explain how a blockchain accumulates blocks, starting from transaction initiation. (7)

OR

14 a) Describe how decentralization of computing or processing power is achieved by a blockchain. (7)

b) What is consensus mechanism in blockchain? List and explain any four types of consensus mechanisms. (7)

Module III

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

b) What is a blockchain wallet? Describe any four types of wallets. (7)

OR

16 a) Explain various steps in transaction validation with respect to Bitcoin. (7)

b) Illustrate the working of Practical Byzantine Fault Tolerance (PBFT). (7)

Module IV

17 a) Give the significance of oracle in smart contracts. Elaborate different type of oracles deployed in blockchain . (7)

b) Explain how blockchain can be applied in health sector. (7)

OR

18 a) What are DApps? Explain the design aspects of DApps. (7)

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

Module V

19 a) Explain the architecture and components of Ethereum ecosystem. (7)

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

OR

20 a) Explain the data types and functions used in Solidity language. (7)

b) Explain how transactions are processed in Ethereum. Also explain the concept of gas and how does it affect the transaction processing? (7)

****