(T) Roll No. .....

PAPER ID—11686

Bachelor of Technology

EXAMINATION, 2025

(Seventh Semester)

COMPUTER SCIENCE AND ENGINEERING

Foundations of Blockchain Technology

Time : 3 *Hours* *Maximum Marks* : 70

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all. Q. No. **1** is compulsory. All questions carry equal marks.

Compulsory Question

1. (a) What is meant by consensus in distributed computing ? 2

   (b) State one important property of a cryptographic hash function used in blockchains. 2

   (c) What purpose does a Merkle tree serve in a cryptocurrency system ? 2

   (d) Mention the role played by the Ethereum Virtual Machine (EVM). 2

   (e) Give a brief meaning of SNARK. 2

   (f) What function does a cryptocurrency wallet perform ? 2

   (g) Write a short note on sidechains in blockchain networks. 2

2. (a) Explain the asynchronous Byzantine agreement problem and discuss its relevance to blockchain consensus. 7

   (b) Describe the GARAY model and explain how it helps analyze the security and reliability of blockchain protocols. 7

3. (a) Discuss how PoW can be analyzed using the random oracle model. 7

   (b) Explain the concept of hybrid blockchain consensus models that combine Proof-of-Work and Proof-of-Stake. 7

4. (a) What properties should a cryptographic hash function satisfy to be suitable for blockchain systems ? 7

   (b) Discuss the role of encryption schemes in securing communication between blockchain participants. 7

5. (a) Describe how Merkle trees enable efficient verification of transactions in Bitcoin. 7

(b) Explain the process of validating a Bitcoin transaction before inclusion in a block. 7

6. (a) Examine how anonymity in Bitcoin is achieved and describe its limitations. 7

(b) Discuss the mathematical relationship between block difficulty, hash rate and average block time. 7

7. Provide a detailed explanation of the architecture and operation of the Ethereum Virtual Machine. 14

8. (a) Discuss common vulnerabilities found in smart contracts and illustrate typical attacks that exploit these weaknesses. 7

(b) Explain the concept of sidechains and describe how they improve scalability and interoperability for Ethereum-based systems. 7

9. (a) What is a zero-knowledge proof ? Discuss its importance in enhancing privacy within blockchain systems. 7

(a) Discuss how blockchain can be integrated into IoT networks and medical record systems to enhance security, trust and tamper-resistance. 7

❖❖❖❖❖❖❖