(T) Roll No. .....

PAPER ID—11185

B.Tech. EXAMINATION, 2024

(Fifth Semester)

COMPUTER SCIENCE AND ENGINEERING

Cryptocurrency with Ethereum

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, selecting *one* question from each Unit. Q. No. **1** is compulsory. All questions carry equal marks.

1. (a) What is the period of a stream cipher with a key stream of 100 bits that is repeated every 20 bits ?

(b) Name the two main types of Bitcoin wallets.

(c) What is the role of private and public keys in a digital signature ?

(d) What property of a cryptographic hash function ensures that it is computationally infeasible to find two different inputs that produce the same output ?

(e) What is the difference between a hot wallet and a cold wallet in Ethereum ?

(f) Who are the key stakeholders involved in the regulation of cryptocurrencies ?

(g) What factors influence the global acceptance of cryptocurrencies ?

2×7=14

Unit I

2. (a) Explain the significance of Bitcoin's introduction in 2009 and how it influenced the development of other cryptocurrencies ? 7

   (b) Elaborate the advantages of Elliptic Curve Cryptography (ECC) in terms of security and efficiency compared to traditional public key cryptographic methods like RSA. 7

3. (a) Describe, how digital signature schemes work in cryptocurrencies and why they are essential for transaction security and authenticity ? 7

   (b) What is the difference between symmetric and asymmetric encryption schemes in the context of cryptocurrency and their applications in securing transactions ? 7

Unit II

4. (a) Describe the life-cycle of a Bitcoin miner, from setting up mining hardware to receiving rewards and maintaining mining operations. 7

   (b) Discuss the advantages of using Merkle Trees in blockchain technology, particularly in ensuring data integrity and efficient verification. 7

5. (a) Justify, how Bitcoin's scripting language facilitates complex transactions, such as multi-signature and time-locks ? 7

   (b) Illustrate, how the decentralized nature of Bitcoin's P2P network prevents single points of failure and enhances security ? 7

Unit III

6. (a) Elaborate the key features of smart contracts on Ethereum, such as immutability and self-execution and their applications in various industries. 7

(b) Describe the construction of the Ethereum network, including the role of miners, nodes and consensus mechanisms. 7

7. (a) Explain some of the common vulnerabilities in Ethereum smart contracts and the possible consequences of these vulnerabilities being exploited. 7

(b) Discuss, how GHOST enhances the security and scalability of the Ethereum blockchain compared to traditional consensus protocols like Bitcoin's Proof-of-Work. 7

Unit IV

8. (a) Analyse the potential economic impact of widespread cryptocurrency adoption on the global economy, focusing on issues such as cross-border payments, inflation, and monetary policy. 7

(b) Compare Bitcoin's scripting language with Ethereum's smart contract functionality. Discuss their differences in terms of flexibility, complexity and use cases. 7

9. (a) Highlight the significance of Bitcoin's whitepaper and how it laid the foundation for the development of blockchain technology and cryptocurrencies ? 7

(b) Explain, how global regulations affect the operation of cryptocurrency exchanges and the implications for businesses and consumers ? 7