W/D/TY

Reg. No: 22BCE3246

VIT
Vellore Institute of Technology

Final Assessment Test – April 2025

Course: BCSE325L - Introduction to Bitcoin
Class NBR(s): 1903/1913/6626
Time: Three Hours
Slot: B1+TB1
Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions
(10 X 10 = 100 Marks)

1. Explain how the Bitcoin blockchain employs SHA-256 to ensure data integrity.

2. Illustrate how the properties of Collision Resistance, Hiding, and Puzzle Friendliness enhance the security of Bitcoin.

3. In the context of the Bitcoin network, evaluate whether each of the following modifications would require a hard fork or a soft fork. Provide justification for your answers:
   i. Introducing a new OP_BLAKE2 script instruction. [2]
   ii. Removing the OP_CHECKMULTISIG instruction. [2]
   iii. Mandating that each block header include the hash of all pending transactions. [3]
   iv. Requiring that all inputs in a transaction be sorted by age in descending order. [3]

4. Suppose you are designing a Bitcoin wallet that uses Pay-to-Script-Hash (P2SH) to implement a multi-signature wallet with a 2-of-3 signing requirement. Describe how you would implement P2SH in this scenario. Explain how the P2SH mechanism applies to the Bitcoin transaction structure and how the script would be validated during the transaction process.

5. Alice is developing a Bitcoin wallet for a financial application. To enhance privacy, she plans to generate a new address for each transaction and adopts Hierarchical Deterministic (HD) wallets based on the Bitcoin Improvement Proposal 32 (BIP32) standard. Using a single master seed phrase, explain how HD wallets enable her to create unique addresses while ensuring wallet recovery. Additionally, describe the role of public and private key derivation paths in this process.

6. Illustrate Shamir's Secret Sharing scheme and explain its role in preventing single points of failure in cryptographic key management.

7.a) The total annual energy consumption of a specific Bitcoin mining facility is estimated to be approximately 70 terawatt-hours (TWh) based on a top-down analysis. The facility operates 1,500 mining rigs, each with an average power consumption of 1,100 watts, running continuously 24/7 throughout the year. Calculate the estimated annual energy consumption of this Bitcoin mining facility in terawatt-hours (TWh) using the bottom-up approach.

OR

b) A Bitcoin mining farm operates 500 Application-Specific Integrated Circuit (ASIC) miners, each with a hash rate of 90 Tera hashes per second (TH/s) and a power consumption of 3,400 watts. The current block reward is 6.25 BTC, and the mining farm contributes 0.01% of the total network hash rate. Electricity costs ₹7 per kilowatt-hour (kWh), and the farm operates continuously, 24/7. Calculate how much Bitcoin the mining farm could earn in a year, assuming it contributes 0.01% of the total network hash rate.

8.a) Explain the purpose of decentralized mixing and how it enhances the anonymity of Bitcoin transactions. Additionally, describe the steps involved in the CoinJoin protocol to improve the anonymity.

OR

8.b) Explain the key features of the Zerocoin protocol and how it differs from Bitcoin's standard transaction system. Discuss how Zerocoin achieves transaction anonymity and ensures privacy while maintaining the integrity of the blockchain.

9. Elucidate the key principles of Proof of Stake and Virtual Mining, highlighting how they differ from Bitcoin's traditional Proof of Work mechanism. Describe how these methods improve energy efficiency and contribute to the scalability of blockchain systems.

10. Explain the concept of Bitcoin as smart property and how it enables the automated transfer of ownership. Discuss the roles of cryptographic keys and smart contracts in ensuring secure and trustless transactions when using Bitcoin as smart property.

⇔⇔⇔ W/D/TY ⇔⇔⇔