X/D/TY

Reg. No: 22BCE3250

VIT
Vellore Institute of Technology

# Final Assessment Test – April 2025

Course: **BCSE325L - Introduction to Bitcoin**

Class NBR(s): **1910/1919**

Slot: **B2+TB2**

Time: **Three Hours**

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. A group of hackers attempts to alter past Bitcoin transactions by modifying old blocks in the blockchain. Discuss how cryptographic hash functions and hash pointers, prevent such an attack. If they were to succeed, what vulnerabilities would exist in Bitcoin's design?

2. David is designing a Bitcoin-based escrow system. He decides to use a multi-signature script. Analyze how Bitcoin scripts enable an escrow system. What type of script would David use, and how does the script ensure fair execution without requiring a trusted third party?

3. A crypto trader notices that their Bitcoin transactions sometimes take hours to confirm, while competitors' transactions are processed within minutes. The trader regularly uses an exchange wallet but is unaware of the fee mechanisms. Explain the role of transaction fees in Bitcoin trading and suggest strategies to optimize transaction speed while minimizing costs.

4. A financial institution wants to store a large amount of Bitcoin for long-term investment. The management is considering either a multi-signature wallet with key splitting or a combination of hot and cold storage. Compare these approaches, highlighting the risks and benefits of each in terms of security, accessibility, and operational complexity.

5. A decentralized finance (DeFi) startup decides to use a threshold signature scheme to manage its Bitcoin treasury. The company splits the private key among five executives, requiring at least three to sign transactions. Discuss the advantages and risks of this approach, including scenarios where it might fail or lead to internal conflicts.

6. A miner successfully solves a block but fails to broadcast it to the network in time due to poor internet connectivity. Another miner solves the next block, causing the first miner's block to become orphaned. Explain the concept of orphan blocks and how they impact mining incentives and network stability.

7. A mining company is considering switching from solo mining to joining a mining pool. They are concerned about centralization risks and reduced rewards due to pool fees. Assess the trade-offs involved in solo mining versus mining pools and how they impact the security of the Bitcoin network.

8. A financial regulator claims that Bitcoin mixing services enable illegal activities and should be banned. However, a privacy advocate argues that mixing is essential for financial freedom. Evaluate the technical and ethical aspects of Bitcoin mixers, considering their role in decentralization and privacy.

9.a) A validator in a PoS-based blockchain has been caught manipulating transactions for personal gain. Unlike PoW, where mining difficulty regulates security, PoS relies on financial incentives. Discuss how PoS addresses such security risks and what penalties can be applied to dishonest validators while ensuring network integrity.

**OR**

9.b) A new blockchain network wants to implement a consensus mechanism that balances security, decentralization, and energy efficiency. The developers must decide between a Proof of Work (PoW)-based puzzle and a Proof of Stake (PoS) virtual mining system. Analyze the key cryptographic puzzle requirements in PoW and explain how PoS replaces computational puzzles with economic security.

10.a) A startup is designing a new blockchain-based lottery system where participants use cryptographic puzzles to fairly generate winning numbers. Considering the essential puzzle requirements, discuss how Bitcoin's proof-of-work mechanism could be leveraged as a randomness source. What challenges might arise in ensuring fairness and security?

**OR**

10.b) A financial institution is considering implementing a blockchain-based audit system to track transactions securely over time. They are debating between Bitcoin's append-only log and a proof-of-stake-based blockchain. Analyze the trade-offs between these two models, focusing on security, energy efficiency, and the risk of historical data manipulation.

⇔⇔⇔ X/D/TY ⇔⇔⇔