BG/K/TY

Reg. No: 22BCE3759

VIT
Vellore Institute of Technology

Course: **Final Assessment Test – November 2025**
BCSE325L - Introduction to Bitcoin
Class NBR(s): 1541/1543
Time: Three Hours
Slot: E1+TE1
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

COs	CO Statements
CO1	Understand the fundamentals of Cryptography.
CO2	Gain knowledge about various operations associated with Cryptocurrency.
CO3	Develop the methods for verification and validation of Bitcoin transactions.
CO4	Apply the principles, practices and policies associated with Bitcoin business.

BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

Answer ALL Questions
(10 X 10 = 100 Marks)

1. a) Explain how cryptographic hash functions can help the company, detect even the smallest change in a record. **[5] CO1 BL2**

   b) Discuss the pre-image resistance, collision resistance and avalanche effect properties that make hash functions suitable for data integrity verification. **[5]**

2. A Bitcoin trader consolidates three unspent outputs of 0.25 BTC (100 blocks old), 0.40 BTC (200 blocks old), and 0.15 BTC (50 blocks old) to create a transaction with two outputs: 0.79 BTC as payment and 0.01 BTC as change. Assume the average network fee rate is 2.8 satoshis. **CO2 BL4**

   a) Calculate the transaction size in bytes. **[2]**

   b) Compute its priority. **[2]**

   c) Determine the minimum fee required. **[2]**

   d) Explain how miners use transaction fees as incentives for validation. **[4]**

3. a) Ravi wants to learn how new blocks are added to Bitcoin. Explain the workflow of Bitcoin mining from transaction creation to block confirmation. **[5] CO3 BL3**

   b) Describe how Proof-of-Work achieves consensus, prevents double spending, and secures the blockchain. Include a labeled diagram showing each stage of mining and consensus. **[5]**

a) A fintech company uses split-key storage for securing Bitcoin, keeping half the key in an online exchange and half in a secure vault. Explain how transaction authorization works in this scheme, discuss the impact of a key compromise on security, suggest key recovery methods, and highlight regulatory considerations for such a hybrid storage solution with an example. [7] CO3 BL3

b) Split the secret value into N=3 shares, such that any K=2 shares can reconstruct the original secret. Choose your own prime number for modulo arithmetic and polynomial coefficients. [3]

5.a) A startup wants to design a custodial wallet platform for corporate clients. Draft a secure key management and transaction authorization model using hot-cold wallet segregation and multi-signature architecture. CO3 BL3

OR

5.b) A cryptocurrency exchange plans to use hot wallets for daily transactions and cold storage for long-term reserves. Explain the differences in accessibility, security, theft risk, and justify which method is suitable for small frequent transactions versus large long-term holdings. CO3 BL3

6. Consider four transactions T1, T2, T3, and T4 included in a block. Construct the Merkle tree and compute the root symbolically using SHA-256 placeholders, explain how a lightweight (SPV) client uses a Merkle proof to verify that T3 is included without downloading the entire blockchain, and discuss the benefits this provides for lightweight clients in terms of verification efficiency and data security. CO3 BL4

7. A cryptocurrency startup is designing its blockchain. Explain the essential requirements of a mining puzzle, why ASIC resistance helps maintain decentralization, and suggest which puzzle features should be prioritized to balance security, miner incentives, and accessibility. CO4 BL3

8.a) Alice claims to know a secret word that opens a locked door in a circular cave, and Bob wants proof without learning it. Explain how the Zero-Knowledge Proof works in this scenario, show a cave diagram, describe completeness, soundness, and zero-knowledge, and discuss its use in privacy-focused cryptocurrencies like Zerocash. CO4 BL4

OR

8.b) Five students Aisha, Rahul, Meena, Priya, and Karan pool their Bitcoins using a CoinJoin transaction to obscure the source of their funds. Explain how CoinJoin enhances each student's privacy compared to individual transactions, discuss the effect if one student refuses to sign, and relate this scenario to a real-world analogy of an anonymous group note exchange to illustrate the privacy principle. CO4 BL4

9.	Rajan is a cryptocurrency miner who has upgraded his hardware and evaluating three mining pool reward schemes: Proportional, Pay-Per-Last-N- Shares(PPLNS) and Pay-Per-Share(PPS). Rajan's mining rig operates consistently throughout the day and he values both predictable income and long term fairness. Based on these considerations, explain how each reward model would affect Rajan's earnings, risk exposure and incentive to remain loyal to a single pool by performing a comparative analysis.	CO4	BL3
10.	Explain how Bitcoin acts as an append-only log, discuss how immutability ensures data integrity, and highlight the benefits of an auditable distributed ledger. Consider secure timestamping in bitcoin and commitcoin.	CO4	BL2

⇔⇔⇔ BG/K/TY ⇔⇔⇔