REG.NO.:

SLOT: E2+TE2

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - 2
FALL SEMESTER 2025-2026

Programme Name & Branch	**: B.Tech. & CSE**
Course Code and Course Name	**: BCSE325L & Introduction to Bitcoin**
Faculty Name(s)	**: Dr. SIVAKUMAR T & Dr. GOPINATH M**
Class Number(s)	**: VL2025260101546, VL2025260101538**
Date of Examination	**: 09.10.2025**
Exam Duration	**: 90 minutes** **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes: (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)
  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

Q.No.	Question	M	CO	BL
1.	a) A Bitcoin trader is consolidating her funds into one transaction by combining three unspent inputs: the first worth 0.25 BTC received 80 blocks ago, the second worth 0.40 BTC received 50 blocks ago, and the third worth 0.15 BTC received 120 blocks ago. From these inputs, she constructs a transaction with two outputs one sending 0.79 BTC to another wallet as payment and the other returning 0.01 BTC to herself as change. i. Calculate the transaction size in bytes. (2M) ii. Compute the transaction priority using the given formula. (2M) iii. Determine if a fee is required, compute the minimum fee the user must pay.(1M)	5	3	3
	b) Suppose Bitcoin is facilitating transactions worth $5,000 per second worldwide, and on average each transaction requires users to hold Bitcoin for 600 seconds. The effective circulating supply of Bitcoin available for transactions is 3 million BTC. i. Using the model, explain how transaction demand links T, D, and S to determine the equilibrium price P. (2M) ii. Calculate the implied price of Bitcoin (P) under this model. Show your steps.(3M)	5		
2.	a) A miner has a hash rate of 1 TH/s, while the Bitcoin network difficulty is 12 trillion. i. Compute the expected number of hashes required to mine a block. (1M) ii. Estimate the average time (in days) this miner would take to find one block. (1M) iii. Comment on the practicality of solo mining under these conditions. (1M)	3	3	3
	b) Consider 4 transactions T1,T2,T3,T4 included in a block. i. Construct the Merkle tree step by step and compute the Merkle root using SHA-256 (symbolically show the concatenation and hashing). (1M) ii. Explain how a lightweight (SPV) client uses the Merkle proof to verify that T3 is included in the block without downloading the entire blockchain. (1M)	2		

Page 1 of 2

VIT
Vellore Institute of Technology

REG.NO.:

SLOT: E2+ TE2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - 2
FALL SEMESTER 2025-2026

	c) Alice prepares a block header of 80 bytes and starts varying the nonce. The target difficulty requires block hashes to start with 18 leading zeros. i. Show how Alice repeatedly hashes the block header with different nonces until the result meets the requirement. (2M) ii. Explain why the "leading zeros" requirement ensures fairness across all miners. (1M) iii. Discuss how difficulty adjustment prevents attackers from exploiting sudden increases in hash power. (2M)	5		
3.	a) Rajan recently upgraded his mining hardware and is considering three mining pool reward schemes: Proportional, Pay-Per-Last-N-Shares (PPLNS), Pay-Per-Share (PPS) i. For each model, analyze Rajan's earnings stability, risk exposure, and fairness. (2M) ii. If Rajan wants predictable daily income with low variance, which pool should he choose and why? (3M)	5		
	b) A miner is working on a proof-of-work system using SHA-256 (m=256). The mining target is T=2^200, and the miner can perform H=10^12 hashes per second. i. Calculate the probability p that a single hash attempt produces a valid nonce. (1M) ii. Calculate the expected number of hashes E[trials] required to find a valid nonce. (2M) iii. Calculate the expected time E[time] in seconds for the miner to find a valid nonce. (2M)	5	3	4
4.	Alice (the prover) claims she knows the secret word that can open a locked door inside a circular cave. The cave has two entrances/exits, A and B, which meet at the locked door in the middle. Bob (the verifier) wants to test Alice's claim without actually learning the secret word. 1. Explain in detail how Alice and Bob can carry out a Zero-Knowledge Proof protocol in this cave scenario. (Include all the steps of interaction.) (3) 2. Draw a neat diagram of the cave to illustrate the process. (3) 3. Clearly describe how the three essential properties of Zero-Knowledge Proofs are satisfied in this example. (4)	10	4	4
5.	a) A group of five university students — Aisha, Rahul, Meena, Priya, and Karan decide to pool their Bitcoin together to obscure the source of their funds before making payments. They agree to use a CoinJoin transaction to enhance privacy. i. Explain how this CoinJoin procedure helps each student increase the privacy of their transaction compared to sending Bitcoin individually. (2M) ii. Suppose one student refuses to sign after seeing the transaction. Discuss how this affects the process and what measures can be taken to ensure cooperation. (1M) iii. Map this scenario to the real-world analogy of a group study session where students exchange notes anonymously to protect privacy, and explain how this analogy helps understand CoinJoin. (2 M)	5	4	3
	b) Priya makes Bitcoin transactions among thousands of similar transactions on the network. Considering what an analyst can and cannot know, explain the concept of an anonymity set, how it protects her privacy, and why probabilities may be applied to better measure her anonymity.	5		

****