REG.NO.: 22BLE0365

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 - I
WINTER SEMESTER 2024-2025

SLOT: B2+TB2

Programme Name & Branch : B.Tech
Course Code and Course Name : BCSE325L and Introduction to Bitcoin
Faculty Name(s) : SATHYARAJ R, JAYAKUMAR S
Class Number(s) : VL2024250501910, VL2024250501919
Date of Examination : 28-01-2025
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s): Answer All Questions

Course Outcomes:
1. Understand the fundamentals of Cryptography.
2. Gain knowledge about various operations associated with Cryptocurrency.

Q. No	Question	M	CO	BL
1.	Define cryptographic hash function. List and explain the essential additional properties that a hash function must possess to be considered cryptographically secure.	10	1	2
2.	Describe the process of constructing a Merkle Tree with 10 transaction for a file stored in a distributed file system, starting from the data blocks and ending with the Merkle Root. Explain how hash pointers are used at each stage of the construction.	10	1	2
3.	In a Bitcoin-based payment system, Alex and Ben are collaborating to purchase a product worth 50 Bitcoin (BTC). Both Alex and Ben have their own Bitcoin wallets, but they decide to merge their funds for a joint payment. Alex contributes 30 Bitcoin, and Ben contributes 20 Bitcoin. Once the combined funds are ready, they initiate the joint transaction to make the payment to the merchant, YOSH Inc. They are using Bitcoin's protocol to ensure that the funds are merged securely for the payment, without the need to rely on traditional financial intermediaries. a. Discuss in detail how Alex and Ben merge their Bitcoin values for a joint payment of 50 Bitcoin. After the payment is made, explain how the system calculates and returns any change to Alex and Ben if their total contribution exceeds the required payment. Explain how the change is structured in the Bitcoin transaction and what happens if Alex and Ben's combined payment exceeds the required amount. b. What security measures are in place to ensure the integrity of the joint Bitcoin payment between Alex and Ben?	6 4	2	2
4.	Explore public keys, signatures, script conditions and how they work together in a Bitcoin transaction. With proper example, how Bitcoin scripts use stack operations to ensure that only the owner with the corresponding private key can authorize a transaction.	10	2	2
5.	Explain the process of Bitcoin transactions using green address and micro payments with suitable examples. List out the merits and demerits of Bitcoin transactions.	10	2	2

****

REG.NO.: 22BLE0365

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 - II
WINTER SEMESTER 2024-2025

SLOT: B2 + TB2

Programme Name & Branch	**: B.Tech**
Course Code and Course Name	**: BCSE325L and Introduction to Bitcoin**
Faculty Name(s)	**: SATHYARAJ R, JAYAKUMAR S**
Class Number(s)	**: VL2024250501910, VL2024250501919**
Date of Examination	**: 17-MARCH-2025**
Exam Duration	**: 90 minutes** **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- Course Outcomes
  - 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 new cryptocurrency investor is exploring ways to store their Bitcoin holdings securely. They are confused between hot and cold storage methods. If you were to explain this concept to a non-technical person, how would you use a real-world analogy to differentiate these storage methods? Provide examples and discuss their trade-offs.	10	CO3	B2
2.	Consider a scenario where a new Bitcoin user wants to send a payment using an online wallet. However, they notice that the transaction is stuck in the mempool due to low transaction fees. • Explain why this happens and suggest two possible ways to resolve it. • What could the user have done differently to avoid this issue?	10	CO3	B2
3.	Imagine you are a Bitcoin miner in a region where electricity costs are rapidly increasing, and government regulations on mining are becoming stricter. You have two choices: • Continue mining but find ways to optimize energy efficiency • Shift to another cryptocurrency that uses a different consensus mechanism Critically analyze both choices and argue which is the more viable long-term strategy. Consider technological, economic, and environmental aspects in your response.	10	CO3	B3
4.	A newly established mining pool aims to attract individual miners but faces challenges in maintaining miner loyalty. What incentive mechanisms can be introduced to ensure miners remain committed to the pool? Discuss both financial and non-financial incentives.	10	CO3	B3
5.	Consider a scenario where Alice makes a Bitcoin transaction, believing she is completely anonymous. Later, she finds out that her transaction history has been traced back to her real identity. • Analyze the potential methods that could have been used to re-identify Alice. • Discuss how blockchain transparency and metadata contribute to reducing anonymity.	10	CO4	B3

****