VIT®

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

REG.NO.:

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2024-2025

SLOT:B1+TB1

Programme Name & Branch	: B.Tech- CSE
Course Code and Course Name	: BCSE325L - Introduction to Bitcoin
Faculty Name(s)	: KATHIRAVAN S , MADHU VISWANATHAM V,SIVAKUMAR
Class Number(s)	: 1913, 1903 ,6626
Date of Examination	: 28-01-2025
Exam Duration	: 90 minutes Maximum Marks: 50

General instruction(s):

- Answer All Questions

.

Q. No	Question	M
1.	Discuss the properties of Digital Signature in Bitcoin Transactions and Explain how ECDSA is utilized for Signature Creation and Verification.	10
2.	Examine and assess the architecture of Scoorge Coin, a hypothetical cryptocurrency. Outline its core components and evaluate the potential weaknesses or constraints associated with its design	10
3.	What is Change Address? Bitcoin isn't based on an account based model. Instead Bitcoin uses a ledger that just keeps track of transactions (transaction based ledger). Explain how does that work with an example? Also explain how it does the joint Payments and Merge payments.	10
4.	a) Alice wants to send 5 BTC from the company's account which is managed by five people. Three signatures are required to pass the transaction. 1. The transaction must include a specific input script that satisfies a particular cryptographic condition. 2. The transaction output script must be a multi-signature script that requires signatures from at least three different private keys. Design the script and evaluate the same	5
	b) Suppose Alice and Bob want to do business with each other. Alice wants to pay Bob in Bitcoins for Bob to send some goods to Alice. The problem is that Alice doesn't want to pay until after she's received the goods, but Bob doesn't want to send the goods until after he has been paid. Provide and explain the suitable solution for this problem through Bitcoin	5
5.	Consider a scenario of Four different people namely A, B, C and D purchased products from a merchant XYZ who is accepting Bitcoin. Discuss the various steps involved with respect to transaction, Blockchain, Merkle tree and digital signature while verifying and validating the transactions. Assume one transaction per block	10