



VIT

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

School of Computer Science and Engineering

Fall Semester 2024-2025 Continuous Assessment Test – I

Programme Name & Branch : B.Tech - CSE

SLOT: F1+TF1

Course Code & Name : BCSE325L –Introduction to Bitcoin

Class Number: 1406

Faculty Name: Madhu Viswanatham V

Exam Duration: 90 Min.

Maximum Marks: 50

General instruction(s):

Answer ALL questions ($5 \times 10 = 50$)

1. Illuminate how SHA-256 works to generate the fixed hash value that act as integrity of the data in Blockchain [10]
2. Alice is having the habit of storing her private key in a single place. So there is a problem of single-point failure and she loses her Bitcoins. Derive a suitable solution to solve the single point failure problem and discuss the solution. [10]
3. What is Merkle root and construct a Merkle tree with 10 transactions and illustrate the steps in data and consistency verification of Merkle tree with appropriate examples. [10]
4. 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 Payment. [10]
5. What happens when the customer purchases with Bitcoin through a payment processing Interface. Illustrate the payment process involving user, merchant and payment service. [10]