REG.NO.:

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: B1+TB1

Programme Name & Branch	: B.Tech Computer Science and Engineering
Course Code and Course Name	: BCSE 325L – Introduction to Bitcoin
Faculty Name(s)	: Sivakumar Nagarajan, Kathiravan, Madhu Viswanatham
Class Number(s)	: VL202450506626
Date of Examination	: 17-03-2025
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)
- 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.	Transparent Exchange claims that it controls at least 500,000 BTC and wants to prove this to its customers. To do this it publishes a list of addresses that have a total balance of 500,000 BTC. It then signs the statement "TransparentExchange controls at least 500,000 BTC" with each of the corresponding private keys and presents these signatures as proof. What are some ways in which TransparentExchange might be able to produce such a proof even if it doesn't actually currently control 500,000 BTC? How would you modify the proof to make it harder for the exchange to cheat?	10	CO3	2
2.	A Bitcoin payment service might receive thousands of payments from various users near-simultaneously. How can it tell whether a particular user Alice who logged into the payment service website and initiated the payment protocol actually made a payment or not?	10	CO3	2
3.	A startup is looking to enter the Bitcoin mining industry and needs to decide on the most cost-effective hardware solution for their operation. They are considering four options: CPU, GPU, FPGA, and ASIC. The startup is operating in an area with high electricity costs and a limited budget for initial investment. They want to maximize efficiency while minimizing ongoing energy expenses. Considering the high electricity costs and the limited budget, which mining hardware (CPU, GPU, FPGA,	10	CO3	3