REG.NO.: 21BCE0374

PRP III - (8)

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
FALL SEMESTER 2024-2025

SLOT:F1+TF1

Programme Name & Branch : B.TECH CSE
Course Code and Course Name : BCSE325L- Introduction to Bitcoin
Faculty Name(s) :V.Madhu Viswanatham
Class Number(s) : 1406
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

Q. No	Question
1.	Is mining in pools more beneficial to Bitcoin coin miners? Compare the ways in which the mining rewards will be distributed to the pool members. How the pool hopping is regulated and explain with suitable scenario? [10]
2.	Imagine a user who frequently transacts in Bitcoin for both personal and business purposes. They are concerned about their transaction history being publicly accessible on the Blockchain. How can they utilize mixing services to enhance their privacy, and what risks should they be aware of? [10
3.	Assess whether the following new features could be added using a hard fork or soft fork. [10] (i).The old Blockchain will continue to accept blocks from the newly updated Blockchain protocol, even though there is a change in the rules because of the new software (ii).A disagreement in the Bitcoin community over the best approach for scaling the network. (iii). A requirement that each miner include a Merkle root of unspent transaction outputs (UTXOs) in each block (iv). A requirement that all transactions have their outputs sorted by value in ascending order (v) . Update in the source code to change the rewards for miners
4.	What is a Blind signature? Illustrate how it helps in the implementation of an anonymous E-cash system [10]
5.	Define a block withholding attack and explain how it affects the overall efficiency of Bitcoin mining pools. What are the long-term consequences of such an attack on the network's stability and profitability? [10]

****