REG.NO.:

VIT

Vellore Institute of Technology

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CONTINUOUS ASSESSMENT TEST - I

WINTER SEMESTER 2024-2025

SLOT: C1

Programme Name & Branch	: B.Tech & BCE, BICT
Course Code and Course Name	: BCSE327L & Smart Contracts
Faculty Name(s)	: Dr. S. Sridevi
Class Number(s)	: VL2024250502184
Date of Examination	: 29-1-2025
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)
- Course Outcomes: CO1: Understand the basics and objectives of Smart Contracts in a Blockchain.
- CO2: Evaluate the various functionalities and features in an Ethereum to generate Smart Contracts.

Q. No	Question	M	CO	BL
1.	A company is looking to implement a smart contract for an automated supply chain system. The contract will trigger payments when a shipment reaches a certain location and automatically update inventory records. What are the important concepts and practices should be aware of while designing the smart contract to ensure the correct flow of information and actions based on external events (e.g., GPS data or sensor inputs)?	10	CO1	BL2
2.	A developer is debugging an issue where users are not able to interact with their deployed smart contracts on Ethereum. To assist in troubleshooting, a developer needs to explain how the Ethereum Virtual Machine processes a transaction that calls a function within a smart contract. Describe the step-by-step process of how the transaction moves through the EVM, including state changes, execution of instructions, and the role of the stack. Provide a detailed diagram to illustrate each phase of the transaction.	10	CO1	BL1
3.	A cryptographer is attempting to analyze the security of a SHA-256 implementation in a network protocol. The data being hashed in the protocol is of varying lengths. How does padding, parsing and hash computation in the SHA-256 algorithm ensure that even small data sets or data with specific bit lengths still produce unique and consistent hash outputs?	10	CO2	BL3
4.	A government agency needs to protect classified data while transmitting it between departments. They are considering using asymmetric encryption for securing communications but are concerned about the speed and computational overhead of the encryption process. How would you explain the difference between symmetric and asymmetric encryption, and which method would be better suited for encrypting large volumes of data efficiently?	10	CO2	BL3
5.	Describe in detail about the role of smart contract in the domains below with examples: 1)Land registration, 2) Retail , 3) Warranties, 4) Supply chain and explain about the details stored in blockchain to preserve the characteristics of application.	10	CO2	BL3

****