Y/D/TY

Reg. No: [redacted]

Final Assessment Test – April 2025

VIT
Vellore Institute of Technology

Course: **BCSE327L - Smart Contracts**

Class NBR(s): **2184** Slot: **C1**

Time: **Three Hours** Max. Marks: **100**

- **KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE**
- **DON'T WRITE ANYTHING ON THE QUESTION PAPER**

Answer ALL Questions

(10 X 10 = 100 Marks)

1. Designing a decentralized application (DApp) for a healthcare organization on the Ethereum platform requires a robust security framework to manage sensitive patient records and prescriptions. The application must restrict access to authorized medical professionals only, while ensuring the integrity of patient data and preventing tampering. What security features of smart contracts should be prioritized to protect patient privacy, ensure data integrity, and prevent unauthorized access?

2. Design how the security of a SHA-256 implementation can be analyzed in a network protocol where the data being hashed has varying lengths. How do 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?

3. Describe how a supply chain company can implement a smart contract solution on Ethereum to automate and track inventory shipments in real-time. The system should automatically trigger actions such as releasing payments once specific milestones, like inventory arriving at a warehouse, are reached. What are the key features of Ethereum smart contracts that make them suitable for automating inventory management, and how do they ensure transparency, efficiency, and trust among different stakeholders (e.g., manufacturers, distributors, and customers)?

4. Discuss in detail about the purpose of using smart contract for the following fields:

   1) Finance, 2) Music and art, 3) Energy, 4) Healthcare, 5) Smart applicants like smart homes, smart cities etc.

   and explain in detail how the aforementioned applications are benefited by using smart contract based DApps.

5. Discuss the future resistance features in smart contract applications and their potential impact on various industries.

6. In a decentralized insurance system, claims are processed automatically based on predefined conditions, with Merkle trees used to verify claim legitimacy and ensure transparency. How would you implement Merkle trees in the smart contract to ensure the integrity and security of claim data? What features would you add to provide transparency in claims and payouts?

7. Discuss about the technologies needed to build Blockchain DAPP with neat sketch, and discuss the connection establishment step between frontend with Blockchain DAPP.

8. Discuss how blockchain technology ensure data permanence in decentralized applications (dApps) by addressing data immutability, decentralization, and storage. Provide examples of dApp use cases that benefit from permanent data storage. Discuss challenges related to storing large data volumes on the blockchain. Speculate on future developments that might address current data storage limitations.

9.a) Imagine a decentralized charity platform where donors contribute to various causes, and the charity organization can withdraw funds upon reaching predefined milestones. Each cause is assigned a unique ID, and the smart contract monitors total donations, milestone achievements, and fund withdrawals. The contract enables donors to contribute, track donations, and ensures that the charity can withdraw funds only when milestone conditions are fulfilled. Additionally, the contract emits events upon donations, milestone achievements, and withdrawals. How would you design state variables within the smart contract to monitor donations, milestones, and withdrawals for each cause, ensuring that funds are withdrawn only upon meeting the specified milestones?

OR

9.b) In a blockchain-based real estate marketplace, property buyers and sellers execute transactions through smart contracts. How would you implement payable functions to facilitate property payments? Also, how would you manage local variables (e.g., individual property sale amounts) and global variables (e.g., total sales volume) within the contract?

10.a) Imagine a development team is building a decentralized application (dApp) comprising multiple interconnected smart contracts. During the testing phase, discrepancies arise in contract interactions and logic. What steps should the team follow to isolate the issues, debug the contracts, and ensure seamless interaction among all smart contracts within the dApp?

OR

10. b) Imagine a decentralized music platform where artists can upload their songs and receive royalties whenever their music is streamed or purchased. The platform uses a smart contract to manage the distribution of royalties. Each song has a unique ID, and the contract keeps track of the number of streams, purchases, and the total royalties earned. The contract should allow the artist to withdraw their earnings and emit events whenever a song is streamed, purchased, or when royalties are withdrawn.

⇔⇔⇔ Y/D/TY ⇔⇔⇔