

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination, December 2023
B. Tech. (CSE), Semester V/VII, 2022-2023

Roll No.....

CS1226: FOUNDATION OF BLOCKCHAIN TECHNOLOGY

Time: 2 hours

Max. Marks: 30

Instructions to students:

1. Do not write anything other than your roll number on question paper.
2. Mention all the assumptions for your answers clearly.

Q. 1.1	Function modifiers play an important role in Solidity. Mention the important modifiers in Solidity with examples.	3.0 (LO2, 4)
Q. 1.2	What does the gas usage in a transaction depends on and how is the transaction fees calculated?	2.0 (LO2, 4)
Q. 1.3	What can a 51% attacker do?	1.0 (LO1)
Q. 2.1	Explore your knowledge and differentiate between the following: - a) Bitcoin and Ethereum b) Ledger and HyperLedger c) Traditional Finance and DeFi	3.0 (LO5)
Q. 2.2	As per synchronous Byzantine model theorem, there is no algorithm to solve consensus if only oral messages are used, unless <i>more than two thirds</i> of the generals are loyal. Create a scenario with $n=4$ and $f=1$ where n stands for number of nodes and f stands for faulty nodes.	3.0 (LO3)
Q. 3.1	Merkle tree is a data structure used in Blockchain. Explain what Merkle tree and its structure is.	3.0 (LO2)
Q. 3.2	Use suitable example to discuss the security properties of Hashing : a) Collision resistant b) Hides the original string c) Puzzle friendly.	3.0 (LO3)
Q. 4.1	Alice's US\$1 is equal to Bob's US\$1, and both of them can swap their US dollar because it has the same value. Justify which type of token it is and what ERC standard it should follow.	2.0 (LO1, 5)
Q. 4.2	What about Stable coins? Are They Coins or Tokens? Give example to justify your answer. How ICO is different from IPO?	2.0 (LO1.6)

Q. 4.3	Explain how visibility and provenance of goods can be assured in a supply chain blockchain with suitable flow diagram.	2.0 (LO 5)
Q. 5.1	Observe the following code and debug the code so that user can buy/sell token from wallet. <pre> pragma solidity >=0.4.22 <0.7.0; contract MyContract { mapping(address=>uint256) public balances; address wallet; constructor (address _wallet) public { wallet=_wallet; } function buytoken() public { // buy a buytoken // send amount to wallet balances[msg.sender]+=1; wallet.transfer(msg.value); } } </pre>	3.0 (LO1)
Q 5.2	Observe the following code and optimize the code so that lesser Gas fees would be taken for executing the code. <pre> pragma solidity ^0.5.12; // Creating a contract contract fellowCoders { // Initializing array coders int[] public coders; // Function to insert values // in the array coders function Numbers() public { coders.push(1); coders.push(2); //Creating a new instance int[] _____ myArray = coders; // Adding value to the // first index of the new Instance myArray[0] = 0; } } </pre>	3.0 (LO1-LO3)