

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination, May 2026
B. Tech. (CSE), Semester VI, 2025-26

Roll No.....

CS1203: Blockchain Technology and Applications

Time: 2 hours

Max. Marks: 30

General Instructions:

1. This paper carries 30 marks. Attempt ALL questions.
2. Do not write anything on question paper except roll no.
2. Marks for each question are indicated in brackets [].
3. Support your answers with diagrams, examples, or calculations wherever applicable.
4. For numerical questions, show all working steps clearly.
5. Answers without justification for Q1 (consultant scenario) will not receive full credit.

Q1.

[10 Marks]

A logistics company, Trade Route Pvt. Ltd., is evaluating whether to adopt blockchain technology to manage its pan-India freight network. The network involves 400+ transporters, 12 regional warehouses, 3 insurance providers, and a central operations team. Currently, disputes over freight delivery confirmation, invoice tampering, and cargo insurance claims take 15–20 days to resolve.

You have been hired as a blockchain consultant. Your task is to:

- (a) Apply the 'Do You Need a Blockchain?' decision framework to this scenario. Evaluate each criterion multiple writers, need for trust, immutability, intermediary removal and justify whether blockchain is appropriate here. [3]
- (b) If blockchain IS suitable, recommend an architecture (permissioned vs permissionless) and a consensus mechanism. Justify your choice considering the number of parties, privacy requirements, and throughput needs. [3]
- (c) Design a high-level smart contract for freight delivery confirmation. Specify at least three contract states (e.g., Dispatched, In-Transit, Delivered), the triggering events, and what data gets recorded on-chain vs off-chain. [2]
- (d) Identify TWO risks of adopting blockchain in this scenario (e.g., oracle problem, 51% attack, regulatory) and propose a mitigation strategy for each. [2]

Q2.

[6 Marks]

(a) Describe the Proof-of-Work (PoW) consensus mechanism. A miner finds a nonce such that: $\text{SHA256}(\text{Block Header} \parallel \text{Nonce}) < \text{Target}$. If the current target requires the hash to begin with 18 leading zeros, explain qualitatively how changing the target to 20 leading zeros affects mining difficulty and network security. [2]

(b) Explain the role of Gas in Ethereum. A Solidity developer wrote the following inefficient contract. Identify the gas-optimisation issues and rewrite the corrected version with a brief explanation for each change made. [2]

```
pragma solidity ^0.8.0;
contract TokenTracker {
    uint256[] public balances;
    string public constant TOKEN_NAME = "MyToken";

    function updateBalances(uint256[] memory newBalances) public {
        for (uint256 i = 0; i < newBalances.length; i++) {
            balances.push(newBalances[i]); // storage write in loop
        }
    }

    function getLength() public view returns (uint256) {
        return balances.length;
    }
}
```

(c) Design assumptions for a hybrid digital payment system combining the strengths of CBDC, UPI, and cryptocurrencies. [2]

Q3.

[10 marks]

- (a) Describe the four-layer architecture of a typical DApp (Frontend → Wallet → Smart Contract – each layer, name the commonly used tool and explain its specific role. Additionally, contrast Hardhat with Truffle as development frameworks, identifying at least advantages Hardhat offers over its predecessor. [3]
- (b) The Walmart E. coli crisis of 2018 exposed the fatal flaws of traditional supply chain databases. Using the six-dimensional comparison (control, editability, auditability, transparency, trust, tracing speed), explain why centralized systems failed and how Hyperledger Fabric-based blockchain reduced traceability time from 7 days to 2.2 seconds. Also describe the role of smart contract logic in automated recall detection. [3]
- (c) The Web3 ecosystem is built on three interconnected pillars DApps (the application layer), DeFi (the financial layer), and DAOs (the governance layer). Using Uniswap as a concrete example that spans all three: (a) explain how Uniswap operates as a DApp (smart contract backend, no central server), (b) explain its DeFi mechanism (Automated Market Maker, liquidity pools, fee distribution), and (c) explain how Uniswap's governance works as a DAO (UNI token voting, protocol upgrade proposals). Conclude by discussing what single point of failure if any remains in this supposedly "fully decentralized" system. [4]

Q4.

[4 Marks]

Merkle Tree & Block Validation

A block contains the following six transactions with their computed hash values:

Tx	Hash Value	Tx	Hash Value
T1	H1 = A3F9	T4	H4 = D2C1
T2	H2 = B7E4	T5	H5 = E9A6
T3	H3 = C1B8	T6	H6 = F3D5

Use the rule: $\text{Parent} = \text{Hash}(\text{Left Child} || \text{Right Child})$. For an odd node, duplicate it to pair with itself.

- (a) Draw the complete Merkle Tree and compute all intermediate hash labels (e.g., $H_{12} = \text{Hash}(H_1 || H_2)$) up to the Merkle Root. [2]
- (b) A lightweight SPV (Simplified Payment Verification) client wants to verify that T3 is included in the block without downloading all transactions. List the minimum set of hashes it needs (the Merkle Proof path) and explain how verification works. [1]
- (c) If an attacker tampers with T5 (changing H5 to X9B2), which nodes in the Merkle Tree are affected? Does the block hash change? Explain. [1]

— End of Question Paper —

CO Mapping: Q1→CS1203.4&5 | Q2→CS1203.1 | Q3→CS1203.5 | Q4→CS1203.2&3

