Daffodil International University

Faculty of Science & Information Technology
Department of Computing and Information System
Final Examination, Summer-2026
Course Code: CIS 331
Course Title: Introduction to Blockchain and Cryptocurrencies

Level: 3 Term: 2

Exam Duration: 2 Hours **Marks: 40**

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1.	(a)	Explain the architecture of a blockchain. In your answer, describe the role of transactions/data, timestamp, previous-block hash, current hash, and the way blocks are linked. Explain how this structure supports a distributed and immutable ledger.	[6]	CO1
	(b)	What is cryptocurrency? Explain how cryptography supports secure digital value exchange. In your answer, describe the roles of public and private keys and explain why a cryptographic hash is useful for data-integrity verification.	[4]	CO1
2.	(a)	Compare Proof of Work (PoW) and Proof of Stake (PoS) in terms of participant selection, resource use, incentives and security, and major performance or decentralization trade-offs. Briefly relate your discussion to the evolution from PoW to PoS.	[5]	CO3
	(b)	A blockchain introduces protocol rules that are incompatible with the old software. Some participants upgrade while others continue with the old rules, and two persistent chains are created. Identify the type of fork and analyze the sequence from protocol upgrade to chain split. Explain how this situation differs from a soft fork and mention two consequences for users or validators. Hard	[5]	CO3
3.	(a)	A scholarship smart contract should release funds only after a student's eligibility is approved. Apply the three stages of a smart contract known as contract generation, contract release, and contract execution - to show how the process would work.	[5]	CO2

(b) Study the following Solidity code and answer accordingly. Identify the pragma statement, contract declaration, state variable, and function. Then explain what happens to the blockchain state when setCount() is successfully executed. [5] CO2

```
pragma solidity ^0.8.0;
contract Counter {
    uint public count;
    function setCount(uint newCount) public {
        count = newCount;
    }
}
```

4. (a) A network of hospitals, diagnostic laboratories, and patients wants a tamper-evident history of medical records and verifiable patient consent while keeping sensitive medical data protected. Design a high-level blockchain-based solution. Show the main participants, what should be kept on-chain versus off-chain, and how access/verification would work. [6] CO4

(b) As part of the above design, specify four regulatory, legal, or security requirements that should be addressed before deployment and explain how the proposed system can respond to them. [You may consider data privacy, cybersecurity, accountability, or the conflict between immutability and the right to correct/delete data.] [4] CO4