Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Tech Artificial Intelligence and Data Science - Semester II- End Examination- April 2025

Subject Code: CTMTAIDS SII P5 EL1 **Date:** 29/04/2025

Subject Name: Blockchain Security and Investigations

Time: 10:30am- 01:30 pm **Total Marks:** 100

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three**	
	(a)	Define hash functions and explain their key properties. Discuss the importance of collision resistance and provide an example of their practical applications.	**08**
	(b)	Describe the Byzantine General's Problem and explain the concept of Zero-Knowledge Proof.	**08**
	(c)	Compare and contrast Proof of Work (PoW), Proof of Stake (PoS), and Proof of Burn (PoB) consensus algorithms.	**08**
	(d)	Differentiate between public and private blockchains, highlighting their advantages and limitations.	**08**
Q.2		**Attempt any three**	
	(a)	Explain how the Elliptic Curve Digital Signature Algorithm (ECDSA) functions. Discuss the advantages of digital signatures in blockchain security.	**08**
	(b)	Define and differentiate between soft forks and hard forks in blockchain networks. Explain why forks occur and how they impact the blockchain ecosystem.	**08**
	(c)	Define blockchain and outline its key features. Enumerate the advantages of blockchain over conventional distributed databases.	**08**
	(d)	Explain the concept of a Sybil Attack and provide a real-world example demonstrating its impact.	**08**
Q.3		**Attempt any three**	
	(a)	Explain the structure and functionality of smart contracts, along with their advantages	**08**
	(b)	Discuss the blockchain reward and the transaction in a blockchain network with an example.	**08**
	(c)	Discuss the common security threats and vulnerabilities in blockchain technology.	**08**

(d) Explain the concept cryptography and explain its significance in modern computing. 08

Q.4 **Attempt any two**

(a) Write short notes on: Difficulty Level and Nakamoto Consensus Protocol. 07

(b) Explain the terms Gas, Gas Limit, and Gas Consumption in blockchain transactions. 07

(c) Discuss a real-world application of blockchain in industries such as healthcare, domain name services, the Internet of Things (IoT), or any area of your choice. 07

Q.5 **Attempt any two**

(a) What are the basic principles of security? Explain active and passive attacks 07

(b) Differentiate between symmetric and asymmetric encryption algorithms 07

(c) Explain the life of a blockchain, chain policy, and energy utilization. 07