NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE, MTech CSE (Cyber Security) and MTech CSE (Data Science)
Course Code:	6CS266ME25
Course Title:	Blockchain Technology
Course Type:	Department Elective-II
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
2	0	2	-	-	-	3

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to:

1. comprehend the structure of a Blockchain networks (BL2)
2. evaluate security issues relating to Blockchain and cryptocurrency (BL3)
3. analyse the applications based on Blockchain technology (BL4)
4. develop and deploy a Web 3.0 application utilizing proxy contracts. (BL6)

Unit	Contents	Teaching Hours (Total 30)
Unit-I	**Introduction to Blockchain:** History, Digital Money to Distributed Ledgers, Design Primitives, Protocols, Security (privacy and security of Blockchain), Consensus, Permissions, Privacy	03
Unit-II	**Blockchain Architecture, Design and Consensus**: Basic crypto primitives: Hash, Signature, Hashchain to Blockchain, Basic consensus mechanisms, Requirements for the consensus protocols, PoW and PoS, Scalability aspects of Blockchain consensus protocols	07
Unit-III	**Permissioned and Public Blockchains**: Design goals, Consensus protocols for Permissioned Blockchains, Hyperledger Fabric, Hyperledger fabric components, Smart Contracts, Chain code design, Hybrid models (PoS and PoW), Ganache-Truffle suite for personalized Ethereum Blockchain	09
Unit-IV	**Proxy Blockchain**: Introduction to Proxy Contracts in Solidity, Why Use Proxy Contracts? Types of Proxy Contracts, Security Considerations in Proxy Contracts, How DeFi Protocols Use Proxy Contracts	04
Unit-V	**Web 3.0 for Decentralized Applications:** Evolution from Web 1.0 → Web 2.0 → Web 3.0, Web 3.0 architecture overview (Blockchain, Smart Contracts, dApps, IPFS), Common security risks: Smart contract exploits, Sybil attacks, MEV	04
Unit-VI	**Recent trends and research issues in Blockchain**: Scalability, secure cryptographic protocols on Blockchain, multiparty communication, FinTech and Blockchain applicabilities.	03

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. Narayanan, Arvind, et al., Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press
2. Wattenhofer, Roger, The science of the blockchain, CreateSpace Independent Publishing Platform
3. Bahga, Arshdeep, and Vijay Madisetti, Blockchain Applications: A Hands-on ApproachVPT
4. Nakamoto, Satoshi, Bitcoin: A peer-to-peer electronic cash system, Research Paper
5. Antonopoulos, Andreas M, Mastering Bitcoin: Programming the open blockchain, OReilly
6. Diedrich, Henning, Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, Wildfire Publishing.

Suggested List of Experiments:

Sr. No	Name of Experiments/Exercises	Hours
1.	To implement digital signature to sign and verify authenticated users. Also, show a message when tampering is detected.	04
2.	To create a blockchain and implement replay attacks on the blockchain.	04
3.	To perform thorough study and installation of Anaconda and Python and perform proof of work (POW) consensus mechanism. Also, notice the changes in mining rewards and nonce requirements.	04
4.	To perform thorough study and installation of Remix IDE and Truffle IDE for deploying Smart Contracts and Decentralized Applications (DApps) and create and deploy a Smart Contract for various applications (At least two).	06
5.	Study of Web 3.0 for designing intelligent smart contracts for any two applications.	04
6.	To write a Solidity contract that implements a distributed ticket sales system. Anybody can create an event (specifying the initial price and number of tickets). Anybody can then purchase one of the initial tickets or sell those tickets peer-to-peer. At the event, gate agents will check that each attendee is listed in the final attendees list on the blockchain. (Ethereum programming)	04
7.	Design a proxy smart contract for any two applications.	04