NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	B.Tech. Computer Science and Engineering
Course Code:	2CSDE93
Course Title:	Blockchain Technology
Course Type:	Departmental Elective
Year of Introduction:	2021-22

Credit Scheme

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

Course Learning Outcomes (CLO):

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

1. summarize the concept of Blockchain technology
2. develop the structure of a Blockchain network
3. evaluate security issues relating to Blockchain and cryptocurrency
4. design the applications based on Blockchain technology

Syllabus: **Total Teaching hours: 30**

Unit	Syllabus	Teaching hours
Unit-I	**Introduction to Blockchain:** Need, Blockchain 1.0 to 5.0, types of blockchain, Generic elements of a blockchain, digital money to distributed ledgers, design primitives, protocols, security, consensus, permissions, and privacy.	05
Unit-II	**Blockchain Architecture, Design and Consensus**: Basic crypto primitives: hash, signature, hash chain to Blockchain, basic consensus mechanisms, requirements for the consensus protocol for permission less environment, PoW, PoS, PoB, PoET, and scalability aspects of Blockchain consensus protocols.	06
Unit-III	**Permissioned and Public Blockchains**: Design goals, Consensus protocols for Permissioned Blockchains, Hyperledger Fabric, Decomposing the consensus process, Hyperledger fabric components, Smart Contracts, Chain code design, Hybrid models (PoS and PoW)	09
Unit-IV	**Blockchain cryptography**: Different techniques for Blockchain cryptography, privacy and security of Blockchain, multi-sig concept	05
Unit-V	**Recent trends and research issues in Blockchain**: Scalability, secure cryptographic protocols on Blockchain, multiparty	05

communication, FinTech and adoption of blockchain technology in various applications.

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

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 Approach, VPT
4. Nakamoto, Satoshi, Bitcoin: A peer-to-peer electronic cash system, Research Paper
5. Antonopoulos, Andreas M, Mastering Bitcoin: Programming the open blockchain, O'Reilly Media, Inc
6. Diedrich, Henning, Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, Wildfire Publishing (Sydney)
7. Draft version of "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press
8. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform

Suggested List of Experiments:

Sr. No.	Practical Title	Hours
1.	To implement to perform digital signature to sign and verify authenticated user. Also, show a message when tampering is detected.	02
2.	To create a blockchain and implement replay attacks on blockchain.	04
3.	To perform thorough study and installation of Anaconda 5.0.1 and Python 3.6 and perform proof of work (POW) consensus mechanism. Also, notice the changes in mining rewards and nonce requirement.	02
4.	To create a cryptocurrency and implement Byzantine Generals Problem in Python.	04
5.	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 any application such as finance, healthcare etc.	02

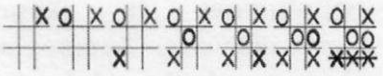
6. To build, implement and test voting mechanism using Ethereum Blockchain. First, list the contestants on the screen and the vote they got. Whenever the user tries to vote a particular contestant, the count of the votes for the particular contestant should increase by 1. Also, the user who has already voted should be marked. Marked means "the user has already voted once and will not be allowed to vote again". 04

7. To perform a thorough study of blockchain development on Hyperledger Fabric using Composer 02

8. To design and develop end-to-end decentralized applications (Dapps). 04

9. 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) 02

10. To write a contract code to implement a two - player game (with a wager on the line) of Tic - Tac - Toe, also known as Noughts and Crosses: (Ethereum programming) 04



Suggested Case List: -NA-