NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	Master of Computer Application (2-Years Programme)
Course Code:	3MCAD356
Course Title:	Blockchain Foundations
Course Type:	Departmental Elective
Year of Introduction:	2021-22

Credit Scheme

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

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

1. define the structure of Blockchain networks
2. apply various models of permissioned Blockchain
3. design the applications based on Blockchain technology
4. evaluate security issues relating to Blockchain and cryptocurrency

Syllabus: **Total Teaching hours: 45**

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	08
Unit-III	**Permissioned Blockchains:** Design goals, consensus protocols for permissioned Blockchains, Hyperledger fabric, decomposing the consensus process, Hyperledger fabric components, chain code design, hybrid models (PoW and PoS)	10
Unit-IV	**Public Blockchain:** Block chains with smart contracts and Turing complete Blockchain scripting – issues of correctness and verifiability	08
Unit-V	**Blockchain cryptography:** Different techniques for Blockchain cryptography, privacy and security of Blockchain, multi-sig concept.	08
Unit-VI	**Recent trends, research issues, and Applications of Blockchain:** Scalability, secure cryptographic protocols on Blockchain, multiparty communication, FinTech and adoption of blockchain technology in various applications	06

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. Imran Bashir, Mastering Blockchain, Packet Publication.
2. Narayanan, Arvind, et al, Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
3. Wattenhofer, Roger, The science of the blockchain, CreateSpace Independent Publishing Platform
4. Bahga, Arshdeep, and Vijay Madisetti, Blockchain Applications: A Hands-on Approach, VPT
5. Nakamoto, Satoshi,Bitcoin: A peer-to-peer electronic cash system
6. Antonopoulos, Andreas M, Mastering Bitcoin: Programming the open blockchain, O'Reilly Media, Inc
7. Diedrich, Henning, Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations, Wildfire Publishing (Sydney)
8. S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, Draft version of 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press.
9. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform.

Suggested List of Experiments:

Sr.	Title	Hours
1	To perform digital signatures to sign and verify authenticated users. Also, show a message when tampering is detected.	02
2	To perform thorough study and installation of Anaconda and Python. Perform proof of work consensus mechanism. Also, notice the changes in mining rewards and nonce requirements	02
3	To create a blockchain and implement replay attacks on blockchain.	04
4	To create a cryptocurrency. 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). Create and deploy a Smart Contract for any application such as finance, healthcare etc.	02
6	To build, implement and test voting mechanisms using Ethereum Blockchain. First, list the contestants on the screen and the vote they got. Whenever the user tries to vote for 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 blockchain development on Hyper ledger Fabric using Composer.	04
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 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)	02

Suggested Case List: -NA-