RAMAKRISHNA MISSION VIDYAMANDIRA

NEP Syllabus B.Sc. Computer Science Honours

Semester-VII

Course Code: 7CMSMJC3

Course Type: Major Course (Elective)

Course Outcome:

- Identify and explain the basics of blockchain technology
- Understand key concepts of private key cryptography and public key cryptography
- Apply the knowledge of blockchain technology in cryptocurrencies and cryptowallets.
- Gain a deep insight into blockchain consensus mechanisms.
- Understand and evaluate Ethereum blockchain, Smart contract and Hyperledger fabric.
- Propose different governmental and non-governmental use cases of blockchain.

7CMSMJC3: Introduction to Blockchain Technology

Credit: 3 **Marks: 50**

Introduction to Blockchain Technology: Introduction, Properties of blockchain, Blockchain myths, Model of decentralization, Distributed ledger, Block header and block in blockchain, Block mining, Block propagation, Blockchain transaction. **[5L]**

Cryptography Primitives: Basic concepts of cryptography, Encryption and decryption using private and public key cryptography, Cryptographic hash function and properties, Hash as message digest, Uses of hash function, SHA-256, Types of hashing, Hash pointer, Markle tree, Construction of hashchain, Blockchain as hashchain, RSA, Digital signature. **[12L]**

Evolution of the Blockchain Technology: Distributed system, Blockchain as distributed system, Distributed consensus, Cryptocurrencies, Evolution of cryptocurrencies, Design goals for cryptocurrencies, Popularity of cryptocurrencies, Cryptowallet, Types of wallets, Desktop wallet, App based wallet, Browser based wallet, Metamask, Transfer of cryptocurrency in metamask, Bitcoin mining, Success of bitcoin as cryptocurrency, Dapps. **[10L]**

Blockchain Consensus: Permissionless models, Permissioned models, Consensus and its challenges, Byzantine fault, Consensus problem, Different consensus mechanisms - Nakamoto consensus (Proof of work), Limitations of Proof of Work (PoW), 51% attack, Proof of Stake (PoS), Proof of Activity (PoAc), Proof of Burn (PoB), Proof of Authority (PoAu), Proof of Elapsed Time (PoET), Proof of Importance (PoI), Ethereum, Go Ethereum, DApps in Ethereum, Ethereum smart contracts (Permissionless Model), Solidity, Two Generals problem, Byzantine Generals problem, Byzantine agreement protocol, Practical Byzantine Fault Tolerance (PBFT), Enterprise blockchain, Hyperledger fabric (Permissioned Model). **[13L]**

Blockchain Applications: Land registry records, Governmental use cases of blockchain, Blockchain for decentralized marketplace, Cross border payments, Know Your Customer (KYC). **[5L]**

7CMSMJC3: Introduction to Blockchain Technology Tutorial

Credit: 1 **Marks: 25**

Exploring real-world blockchain platforms, Exploring blockchain blocks using blockchain explorers, Solving problems on blockchain-related cryptographic algorithms, Demonstration of blockchain-related cryptographic primitives using CrypTool2, Visualisation of Merkle tree, Installation and configuration of MetaMask wallet, Case-study based consensus simulations. **[30L]**

Recommended Books

1. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress.
2. The Science of the Blockchain by Roger Wattenhofer, Inverted Forest Publishing.
3. Mastering Bitcoin: Programming The Open Blockchain by Andreas M. Antonopoulos, Shroff/O'Reilly.
4. Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press
5. Cryptography and Network Security by Behrouz A. Forouzan, McGraw Hill.
6. Cryptography and Network Security: Principles and Practice by William Stallings, Pearson.