Blockchain Technology

Code: CS32223CS	Course Type: Elective	Semester: II
Evolution Scheme (TA-MSE-ESE): 20-30-100	Total Marks: 150	L-T-P (Credits): 3-0-0 (3)

Pre-Requisites: Cryptography, Basic knowledge of computer security, Networking.

Course Objectives:

1. To demonstrate a familiarity with the concepts related to blockchain technology.
2. To apply the knowledge of cryptography and distributed systems to design decentralized applications.
3. To design and build smart contracts and distributed applications (DApps) for different applications.
4. To analyse and explore the real-world applications of blockchain technology.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Students will be able to explain the core concepts and components of blockchain technology.
CO-2	Students will be able to design and implement basic blockchain architectures and understand the security and consensus mechanisms required for their development
CO-3	Students will be understand smart contracts, their technical capabilities, practical applications, limitations and security constraints
CO-4	Students will be able to analyse and explore the Real-World applications of blockchain technology.

Course Articulation Matrix:

PO	PEO-1	PEO-2	PEO-3	PEO-4	PEO-5
CO-1	3	2	1	-	-
CO-2	3	2	1	-	1
CO-3	3	2	-	-	3
CO-4	3	2	1	1	-

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Introduction to Blockchain

Introduction to Blockchain and Digital Currency, Cryptographic primitives, Zero-Knowledge Hash Functions, Evolution, Blockchain as public ledger, Structure of a Block, Transactions, Merkel Trees, Peer-to-Peer Networks, Blockchain Architecture, Types of Blockchain, Characteristics, Benefits and Challenges, Double Spend Problem, Byzantine Generals problem.

Unit-2: Consensus Algorithm and Smart Contract

ConsensusAlgorithms: Proof of Work (PoW), Hashcash PoW, Bitcoin PoW, Attacks on PoW and monopoly problem, Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Byzantine Fault Tolerance (BFT), Proof of Burn, Proof of Elapsed Time, Proof of History (PoH), Leader based Consensus Mechanism: Paxos, Raft. Smart Contract, Applications of Smart Contracts, Mining, Hardness of Mining.

Unit-3: Ethereum and Hyperledger

Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, Using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts, Ethereum Virtual Machine (EVM), Wallets for Ethereum, Solidity, Hyperledger fabric, the plug and play platform and mechanisms in permissioned blockchain, Hyperledger Fabric components, Hyperledger Composer, Corda, Chaincode, Design a Distributed Application (DAPP).

Unit-4: Security and Real World Applications

Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, attacks on Blockchains – such as Sybil attacks, selfish mining, 51% attacks, advent of algorand, and Sharding based consensus algorithms, Blockchain Applications: Cryptocurrencies, Healthcare, Financial system, Supply chain management, E-governance, Real-Estate, Judiciary Micropayments, InsuranceSidechains, Agriculture, Cross-chain interoperability, DeFi & NFTs.

Learning Resources:

Text Books:

- Draft version of "S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, 'Blockchain Technology: Cryptocurrency and Applications', Oxford University Press, 2019.
- Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.
- "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher, Apress.
- "The Basics of Bitcoins and Blockchains" by Antony Lewis, O'Reilly Media.