CS320: Blockchain and Applications	L	T	P	Algorithms and Data Structures
	3	1	0	

Course Objective: To provide an understanding of blockchain technology, distributed ledger systems, consensus mechanisms, and their real-world applications.

S. No	Course Outcomes (CO)
CO1	Describe the fundamental concepts of distributed databases and cryptographic principles used in blockchain technology[Remembering]
CO2	Explain the advantages of blockchain over conventional distributed databases and identify blockchain networks' key components and mechanisms.[Understanding]
CO3	Apply cryptographic techniques such as hash functions and digital signatures to secure transactions within a blockchain network.[Applying]
CO4	Analyze various consensus algorithms and evaluate their effectiveness in maintaining the security and integrity of blockchain networks.[Analysing]
CO5	Develop a simple blockchain application and design smart contracts using Ethereum, addressing potential vulnerabilities and ensuring secure transactions.[Creating]

S. No	Contents	Contact Hours
UNIT 1	Need for Distributed Record Keeping and Consensus algorithms: Modeling faults and adversaries, Byzantine Generals problem, Consensus algorithms and their scalability problems, Why Nakamoto Came up with Blockchain based cryptocurrency.	10

UNIT 2	Blockchain Technologies: Technologies Borrowed in Blockchain — hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash, Atomic Broadcast, Consensus, Byzantine Models of fault tolerance.	**8**
UNIT 3	Cryptographic Foundations of Blockchain: Hash functions, Puzzle friendly Hash, Collision-resistant hash, digital signatures, public key crypto, verifiable random functions, Zero-knowledge systems.	**8**
UNIT 4	Bitcoin Blockchain and Alternatives: Bitcoin blockchain, the challenges, and solutions, proof of work, Proof of stake, alternatives to Bitcoin consensus, Bitcoin scripting language and their use.	**10**
UNIT 5	Ethereum, Smart Contracts, and Advanced Blockchain Concepts: Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages, Verification challenges, Using smart contracts to enforce legal contracts, Comparing Bitcoin scripting vs. Ethereum Smart Contracts, Hyperledger Fabric, Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, Attacks on Blockchains: Sybil attacks, selfish mining, 51% attacks, Advent of Algorand, Sharding-based consensus algorithms	**12**
	Total	**48**