

# CSE436:BLOCKCHAIN

L:3 T:0 P:2 Credits:4

**Course Outcomes:** Through this course students should be able to

- CO1 :: understand blockchain technology and the role of decentralization in blockchain
- CO2 :: discuss the key concepts of symmetric cryptography and public key cryptography
- CO3 :: analyze consensus algorithms and understand the concept of bitcoin
- CO4 :: explore bitcoin network payments, Bitcoin Clients and APIs
- CO5 :: demonstrate smart contract templates, alternative coins, and build smart contracts
- CO6 :: use of truffle for testing, compiling and deployment of smart contracts

## Unit I

**Introduction to Blockchain** : the growth of blockchain technology, the history of blockchain and Bitcoin, distributed systems, blockchain, consensus

**Decentralization** : decentralization using blockchain, methods of decentralization, routes to decentralization, blockchain and full ecosystem decentralization, pertinent terminology, platforms for decentralization, innovative trends

## Unit II

**Symmetric Cryptography** : working with the openssl command line, introduction, cryptographic primitives, Advanced Encryption Standard (AES)

**Public Key Cryptography** : asymmetric cryptography, cryptographic constructs and blockchain technology

## Unit III

**Consensus Algorithms** : introducing the consensus problem, analysis and design, classification, algorithms, choosing an algorithm

**Introduction to Bitcoin** : bitcoin — an overview, cryptographic keys, transactions, blockchain, mining

## Unit IV

**The Bitcoin Network and Payments** : the bitcoin network, wallets, bitcoin payments, innovation in bitcoin, advanced protocols, bitcoin investment and buying and selling Bitcoin

**Bitcoin Clients and APIs** : bitcoin client installation, experimenting further with bitcoin-cli, bitcoin programming

## Unit V

**Alternative Coins** : introducing altcoins, theoretical foundations, difficulty adjustment and retargeting algorithms, bitcoin limitations, extended protocols on top of bitcoin, development of altcoins, Initial Coin Offerings (ICOs)

**Smart Contracts** : history, definition, ricardian contracts, smart contract templates, oracles, deploying smart contracts, the DAO

## Unit VI

**Ethereum 101** : ethereum – an overview, the ethereum network, components of the ethereum ecosystem, Ethereum Virtual Machine (EVM), smart contracts, ethereum development environment

**Further Ethereum** : blocks and blockchain, wallets and client software, nodes and miners, APIs, tools, and DApps, supporting protocols, programming languages

**Introducing Web3** : contract deployment, exploring Web3 with Geth

## List of Practicals / Experiments:

### Integrated Development Environments (IDEs) for Smart contract

- MetaMask and Remix IDE to deploy a smart contract.

### MetaMask in private net

- Adding a custom network to MetaMask and connecting Remix IDE with MetaMask.

**Smart contract with Solidity**

- Write an Ethereum smart contract using solidity.

**Contract Deployment**

- Deploying a contract with MetaMask.

**MetaMask and Remix IDE in contract**

- Interacting with a contract through MetaMask using Remix IDE.

**Use of Geth**

- Installation of Ethereum clients and Ethereum account management using Geth.

**Genesis Block**

- Creation of Genesis Block in Geth.

**Text Books:**

1. MASTERING BLOCKCHAIN A DEEP DIVE INTO DISTRIBUTED LEDGERS, CONSENSUS PROTOCOLS, SMART CONTRACTS, DAPPS, CRYPTOCURRENCIES, ETHEREUM, AND MORE by IMRAN BASHIR, PACKT PUBLISHING

**References:**

1. BLOCKCHAIN TECHNOLOGY: CONCEPTS AND APPLICATIONS by KUMAR SAURABH, ASHUTOSH SAXENA, WILEY