Blockchain Technology

Course Syllabus

Prepared By:	Roshan Singh (Assistant Project Engineer, IIT Guwahati)
Email:	roshansingh3000@gmail.com

Course Outline: Blockchain technology has emerged as a disrupting technology over the last 2 years. With its potentials to solve real-life problems being faced today the technology has attracted huge interests from both academia as well as the industries. The concept and applications of Blockchain has now spread from cryptocurrencies to various other domains, including business process management, smart contracts, IoT, and so on. The course structure has been designed to provide the participants a sound theoretical knowledge as well as hands-on practical experience on formulating and developing blockchain-based DApps. The entire course timeline has been divided into theory as well as practical sessions.

A. Introduction to Blockchain Technology:

Theory:

1. *Opening Lecture:* Providing an intuition, objectives and importance of the course. (1 X 2 = 2 Hrs.)
2. *Introduction to Cryptography I:* Definition of Cryptography, Security goals (CIA Triad), Security services and mechanism, Prime Numbers, Modular Division, Encryption and Decryption, Types of Ciphers(Substitution, Transportation, Stream, and Block) (1 X 2 = 2 Hrs.)
3. *Introduction to Cryptography II:* Group, Fields, and Rings, Symmetric and Asymmetric Cryptography, Public Key Infrastructure, Brief introduction to AES and DES, RSA Algorithm (1 X 2 = 2 Hrs.)
4. *Hashing and Digital Signature :* Properties of hash functions, Message Authentication Code, Secure Hash Algorithm(SHA 256), Digital Signatures, Need for Digital Signatures, Elliptic Curve Digital Signature Algorithm (ECDSA) (1 X 2 = 2 Hrs.)
5. *Fundamentals of Blockchain Technology :* Definition of Blockchain, Properties of Blockchain, Types of System(Centralised, Distributed, Peer-to-Peer, Decentralized), CAP Theorem, Distributed Ledgers & Blockchain, Components of Blockchain(Blocks, Block Header, Block Pointer), Types of Blockchain, in brief, Identifying the need of Blockchain, Applications of Blockchain Technology (FinTech, IoT, Agriculture), Smart Contracts. (1 X 2 = 2 Hrs.)
6. *Consensus Mechanism:* Need for having a consensus mechanism, 3 Generals Problem, Impossibility Theorem, Types of consensus mechanism (Challenge-Response Based, Voting Based), Proof-of-Work, Mining and Incentives, Proof-of-Authority, Proof-of-Stake, Practical Byzantine Fault Tolerance (PBFT), Attack Models on Consensus Mechanism. (1 X 2 = 2 Hrs.)
7. *Bitcoin and Cryptocurrencies:* Definition of cryptocurrencies, cryptocurrencies v/s digital cash, History of Bitcoin, Properties of Bitcoin, Economics of Bitcoin, Roles of Bitcoin Exchanges, Wallets, and its types(Hot, Cold, and Paper), Wallet Security, Bitcoin v/s Altcoins, UTXO Model.(1 X 2 = 2 Hrs.)

Practical:

1. Implement Encryption & Decryption using Ceaser Cipher Algorithms. (1 X 2 = 2 Hrs.)
2. Implement Rijndael algorithm logic. (1 X 2 = 2 Hrs.)
3. Implement Encryption & Decryption using DES Algorithm. (1 X 2 = 2 Hrs.)
4. Implement Encryption & Decryption using RSA Algorithm. (1 X 2 = 2 Hrs.)

5. Implement Message Authentication Code. (1 X 2 = 2 Hrs.)

B. Blockchain Platforms:

Theory:

1. Types of Blockchains: Details and Discussions on the platform
   (a) *Public Blockchains :* (Ethereum): Introduction to Ethereum Blockchain, State Transition Model, Ethereum Virtual Machine(EVM), Accounts, Concept of Gas, Gas Price, Gas Limit, Ethereum TestNets(Rinkeby, Kovan), Ethereum MainNet, Ethash, clique, Casper Ethereum PoS, Difference between Ethereum and Bitcoin, Application of Ethereum beyond cryptocurrencies.(4X2 = 8 Hrs.)
   (b) Private Blockchain: (Hyperledger): Introduction to Hyperledger projects in brief. (1X2 =2 Hrs.)
   (c) Consortium Blockchain (R3 Corda): Introduction to R3 project in brief. (1 X 2 = 2 Hrs.)
2. Use Cases of Ethereum Blockchain: (uPort, SlockIt, Crypto-kitties, Augur, etc.) (2 X 2 = 4 Hrs.)

Practical:

1. Setting up a private, permissioned blockchain network on the Ethereum blockchain platform.(1 X 3 = 3 Hrs.)

C. Smart Contracts:

1. Introduction to Solidity: Background of Solidity, variables, storage, memory, messages, stack operations, mappings other basic constructs. (3 X 2 = 6 Hrs.)
2. Standard Development Tools and libraries: Remix IDE, Truffle, Ganache, Metamask, web3.js. (2 X 2 = 4 Hrs.)
3. Attacks on Smart Contracts: DAO Attack and Parity Hack. (1 X 2 = 2 Hrs.)
4. Best Practices while writing smart contracts. (1 X 2 = 2 Hrs.)

Practical:

1. Mini Project (3 X 2 = 6 Hrs.)

D. DApp Development

Theory:

1. Formulating the problem for the DApp project with proper flowcharts and diagrams following software engineering principles. (2 X 2 = 4 Hrs.)
2. Learning Front End Technologies required for the project(React, HTML, JS, etc) (2 X 2 = 4 Hrs.)

Practical:

1. Major Project (6 X 2 = 12 Hrs.)