DISCIPLINE SPECIFIC ELECTIVE COURSE: Blockchain and its Applications

Credit distribution, Eligibility and Pre-requisites of the Course

Course title & Code	Credits	Credit distribution of the course			Eligibility criteria	Pre-requisite of the course (if any)
		Lecture	Tutorial	Practical/ Practice		
DSE8c: Blockchain and its Applications	**4**	**3**	**0**	**1**	Pass in Class XII	A course in any Programming Language, Database Management Systems

Course Objective

This course covers the basic concepts behind blockchain and presents Bitcoin and other cryptocurrencies as the motivation for blockchain technologies. It provides a substantive discussion about different technologies behind blockchain and cryptocurrencies.

Course Learning Outcomes

On successful completion of the course, students will be able to:

1. understand the applications of blockchain in different domains
2. learn the practical applications of cryptocurrency such as Bitcoin and Ethereum
3. understand basic technologies like cryptographic hash functions, blocks, merkel trees, elliptic curve cryptography and digital signatures.
4. to have knowledge of decentralized consensus algorithms like proof of work, proof of stack, proof of capacity etc.
5. to learn how to record transactions in blockchain, computing bitcoin address etc.
6. to learn about smart contracts and their applications
7. to learn about permissioned and permission less blockchain and hyperledgers.
8. to gain knowledge of real world aspects of Bitcoin, such as wallets and mining techniques. with the Bitcoin network.

Syllabus

Unit 1 Introduction: History of money, Digital Currencies, Ledgers, Cryptography, Centralized and Decentralized systems, peer to peer systems, the purpose of Blockchain, types of blockchain (public, private and semi-private blockchain), application of blockchain (in government, healthcare, real estate, voting, insurance, non-fungible tokens, metaverse, Web 3.0).

Unit 2 Cryptocurrency and Design: Concept of cryptocurrency, History of Bitcoin, concept of mining, challenges of blockchain/bitcoin design (performance, scalability, efficiency, security, governance, public policy and legal framework).

Unit 3 Blockchain Technology: Properties of hash functions, Cryptographic hash functions, hashes (as names, references and commitments), Blocks, Block Headers, Merkel Trees, chain forks, Asymmetric Cryptography, Digital signatures.

Unit 4 Decentralized Network Consensus: Introduction to decentralized networks, Native Currency, consensus, proof of work (PoW), proof of stake (PoS), proof of capacity (PoC), proof of burn (PoB), Practical Byzantine Fault Tolerance (pBFT), Proof of Elapsed Time (PoET).

Unit 5 Permissioned and Permissionless blockchain: Blockchain systems vs. traditional databases, introduction to permissioned/permissionless blockchains and their applications, Advantages and disadvantages, Solidity.

Unit 6 Blockchain and Money Transactions: Satoshi and Bitcoin, Recording of transactions in blockchain, transaction inputs, outputs and format, Bitcoin address.

Unit 7 Smart contracts (Ethereum and other currencies): Overview of smart contracts, tokens and Ethereum as a platform for smart contracts, blockchain technology as regulatory authority.

References

1. Imran Bashir *Mastering blockchain Distributed ledger technology, decentralization, and smart contracts explained*, 2nd edition, Packt Publication, 2018.
2. Lorne Lantz and Daniel Cawrey *Mastering Blockchain Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications*, 1st edition, O'Reilly Publication, 2020.
3. Chris Dannen *Introducing Ethereum and Solidity Foundations of Cryptocurrency and Blockchain Programming for Beginners* ,1st edition, Apress Publication, 2017.

Additional Reference

(i) Daniel Drescher *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, 1st edition, Apress Publication, 2017.

Suggested Practical List

Use any programming language to implement the following:

1. Using SHA256, obtain the message digest of string "Blockchain Developer".
2. Write a program to encrypt and decrypt the message "Hello World" using SHA256.
3. Implement RSA cryptographic algorithm.
4. Create a simple blockchain using Proof of Work (PoW).
5. Demonstrate sending of a digitally signed document.
6. Create a blockchain block containing block hash, transaction history, time of creation.
7. Create a blockchain having 5 nodes and print the hash values of each block.
8. Create a blockchain having 5 nodes and check its validity.
9. Implement a smart contract using solidity programming language.
10. Create a simple permissioned blockchain using Hyperledger Fabric.