DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
KATHMANDU UNIVERSITY

Subject: BLOCKCHAIN TECHNOLOGY[Elective]
Course Code: COMP 492
Credit: 3 F.M: 100

Course Description:

This course deals with fundamentals, applications, and research of blockchain technologies.
It provides a basic introduction to blockchain and its underlying cryptographic protocols followed by the exploration and implementation of blockchain technology applications. Furthermore, it also provides an overview of the current research trends and the future.
.

Course *Objectives:*

1. To understand the concepts of blockchain technology and underlying cryptography
2. To implement the techniques of blockchain to various applications
3. To understand the current research and trends in blockchain domain

Prerequisites:

This course requires earlier knowledge of calculus, linear algebra and computer networks. Prior experience of programming in Javascript will be helpful.

EVALUATION:
Internal: 50
External: 50

Contents:

Unit 1 – Introduction to cryptography [4 hrs]

1.1 Symmetric encryption techniques
1.2 Asymmetric encryption techniques
1.3 Hash functions and its methods
1.4 Digital Signatures and its methods

Unit 2 – Computer networks [3 hrs]

2.1. P2P network
2.2. Distributed Networks

2.3 Consensus Algorithm (Proof of work, Proof of stake, Proof of Authority)

Unit 3 – Blockchain [7 hrs]

3.1 Blockchain technology
- 3.1.1. Decentralization
- 3.1.2. Distributed Ledger Technologies
- 3.1.3. Types of blockchain

3.2 Transactions and Blocks
3.3 Digital Wallets
3.4 Blockchain Nodes & Its Types
3.5 Blockchain based mining
3.6 Implementing bitcoin network using bitcoin RPC
- 3.6.1 Installing bitcoin Core & Setting up a **private** bitcoin network.
- 3.6.2 Creating wallets.
- 3.6.3 Creating transactions.
- 3.6.4 Mining.

Unit 4 – Ethereum Network [6 Hrs]

4.1 History
4.2 Architecture of Ethereum
4.3 Bitcoin vs. Ethereum
4.4 Layered structure of Ethereum
- 4.4.1 Data layer → account generation, transactions, genesis block, uncle blocks, Ethereum world state, gas fee, ether units
- 4.4.2 Consensus Layer → proof of work, forking, DAG file, mining concepts, proof of stake
- 4.4.3 Execution Layer → smart contracts, Ethereum virtual machine
- 4.4.4 Common Layer → Ethereum P2P network, network discovery protocol, Ethereum database, RLP encoding.
- 4.4.5 Application Layer → DAPP, Swarm (P2P file system), whisper (P2P messaging system)

Unit 5 – Applications of Blockchain [15 Hrs]

5.1 Web 1.0 vs Web 2.0 vs Web 3.0
5.2 Use cases of Blockchain → Finances, Supply Chain, Origin & Provenance, Law
5.3 Decentralized Applications and Its Architecture
5.4. Smart Contracts
- 5.4.1. Programming in Solidity
- 5.4.2. Deploying Smart Contracts
- 5.4.3. Smart contract vulnerabilities

5.5. Crypto tokens and their types (ERC-20, ERC -721, ERC-1155)
5.6. Other Applications (blockchain explorer, blockchain DNS, node geolocation)

5.7. Introduction to the Darknet and Misuse of Blockchain (Silkroad, Mt. Gox)
5.8. Bitcoin and Cryptocurrencies in the context of Nepal

Unit 6 – Research on Blockchain technology [10 Hrs]

6.1. Create a curated list of papers on blockchain to inform students of the current research on blockchain. Topics related to scalability and security.
6.2 Students will be asked to present on the papers assigned and will be peer- evaluated.

Text Book:

1. The Blockchain Developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects*, Elad Elrom, Apress, 2019.*

Reference books:

2. The Book of Satoshi: The Collected Writings of Bitocoin Creator Satoshi Nakamato, 1'st Edition, *Phil Champagne*, LLC, 2015.
3. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, *Don Tapscott and Alex Tapscott, 2016.*
4. .Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond, *Chris Burniske and Jack Tatar, 2017*
5. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers them (Cryptography, Derivatives, Investments, Futures Trading, Digital Assets, NFT), *Antony Lewis, 2021*.