ACOMVAC08 BLOCKCHAIN TECHNOLOGY

LEARNING OBJECTIVES

LO1 : By the end of the course, students will be able to Understand how block chain systems (mainlyBit coin and Ethereum) work,
LO2 : To securely interact with them,
LO3 : Design, builds, and deploy smart contracts and distributed applications,

COURSE OUTCOMES

C01: Explain design principles of Bit coin and Ethereum. CO2: Explain Nakamoto consensus.
CO3: Explain the Simplified Payment Verification protocol.
CO4: List and describe differences between proof-of-work and proof-of-stake consensus.
CO5: Interact with a block chain system by sending and reading transactions.
CO6: Design, build, and deploy a distributed application.

UNIT I: INTRODUCTION TO BLOCK CHAIN:

Distributed Database - Two General Problem, Byzantine General problem and Fault Tolerance, Hadoop Distributed File System - Distributed Hash Table, ASIC resistance, Turing Complete - Cryptography: Hash function - Digital Signature - ECDSA, Memory Hard Algorithm, Zero Knowledge Proof.

UNIT II: BLOCK CHAIN SYSTEMS:

Introduction - Advantage over conventional distributed database - Block chain Network - Mining Mechanism - Distributed Consensus - Merkle Patricia Tree - Gas Limit, Transactions and Fee, Anonymity - Reward, Chain Policy - Life of Block chain application - Soft & Hard Fork - Private and Public block chain.

UNIT III: DISTRIBUTED CONSENSUS:

Nakamoto consensus - Proof of Work - Proof of Stake - Proof of Burn - Difficulty Level - Sybil Attack - Energy utilization and alternate.

UNIT IV: CRYPTO CURRENCY AND STRATEGY :

History - Distributed Ledger - Bit coin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract - GHOST, Vulnerability, Attacks, Side chain, Namecoin.

UNIT V: CRYPTO CURRENCY REGULATION:

Stakeholders - Roots of Bit coin, Legal Aspects-Crypto currency Exchange - Black Market and Global Economy - Applications: Internet of Things - Medical Record Management System - Domain Name Service and future of Block chain. Tutorial & Practical: Naive Block chain construction - Memory Hard algorithm – Hash cash implementation - Direct Acyclic Graph, Play with Go ethereum, Smart Contract Construction - Toy application using Block chain - Mining puzzles

TEXT BOOK

1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Gold feder, Bitcoin and Crypto currency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).

SUPPLEMENTARY BOOKS

1. Antonopoulos, Mastering Bit coin: Unlocking Digital Crypto currencies
2. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
3. DR. Gavin Wood, “ETHEREUM: A Secure Decentralized

Transaction Ledger,”Yellow paper.2014.

1. Nicola Atzei, Massimo Bartoletti, and TizianaCimoli, A survey of attacks on Ethereum smart contracts