RASHTRASANT TUKADOJI MAHARAJ NAGPUR UNIVERSITY, NAGPUR
FOUR YEAR BACHELOR OF TECHNOLOGY (B. Tech..) DEGREE COURSE

SEMESTER: Sixth (C.B.C.S.)

BRANCH: COMPUTER SCIENCE & ENGINEERING

Subject: **Open Elective 1: Block-chain Technologies** Subject Code: **BTECH-CSE-604.3T**

Load	Credits	College Assessment Marks	University Evaluation	Total Marks
36 Hrs.	**3**	**30**	**70**	**100**

Aim: To make students aware of Block Chain Technology and how it works. T

Prerequisites: Data Structures and algorithms and basic knowledge of Cryptography.

Course Objectives:

1	To teach the concepts of blockchain technologies.
2	To cover the technical aspects of crypto currencies, block chain technologies, and distributed consensus.
3	To familiarize potential applications for Bit coin-like crypto currencies
4	To learn, how these systems work and how to engineer secure software that interacts with the Bit coin network and other crypto currencies.

Course Outcomes:
Students would be able to:

1	Understand emerging abstract models for Block chain Technology
2	Analyse the concept of cryptocurrency and mathematical background behind it
3	Apply the tools for understanding the background of bitcoins
4	Identify major research challenges and technical gaps existing between theory and practice in crypto currency domain
5	Understanding of latest advances and its applications in Block Chain Technology

SYLLABUS:

UNIT- I:

Introduction Basic of Blockchain Architecture – Challenges – Applications – Block chain Design Principles -The Blockchain Ecosystem - The consensus problem - Asynchronous Byzantine Agreement - AAP protocol and its analysis, Abstract Models for BLOCKCHAIN - GARAY model - RLA Model - Proof of Work (PoW) as random oracle - formal treatment of consistency, liveness and fairness - Proof of Stake (PoS) based Chains - Hybrid models (PoW + PoS)

UNIT-II:

Cryptographic Fundamentals Cryptographic basics for crypto currency - a short overview of Hashing, cryptographic algorithm – SHA 256,signature schemes, encryption schemes and elliptic curve cryptography- Introduction to Hyperledger-Hyperledger framework - Public and Private Ledgers.

UNIT- III:

Bit Coin Bit coin - Wallet - Blocks - Merkley Tree - hardness of mining - transaction verifiability - anonymity - forks - double spending - mathematical analysis of properties of Bit coin. Bitcoin blockchain, the challenges, and solutions, proof of work, Proof of stake, alternatives to Bitcoin consensus, Bitcoin scripting language and their uses.

UNIT- IV:

Ethereum Ethereum - Ethereum Virtual Machine (EVM) - Wallets for Ethereum - Solidity - Smart Contracts - some attacks on smart contracts. Ethereum and Smart Contracts- The Turing Completeness of Smart Contract Languages and verification challenges- comparing Bitcoin scripting vs. Ethereum Smart Contracts

UNIT- V:

Block Chain-Recent Trend Blockchain Implementation Challenges- Zero Knowledge proofs and protocols in Block chain - Succinct non interactive argument for Knowledge (SNARK) - pairing on Elliptic curves – Zcash - attacks on Blockchains

Text Books:

1. Melanie Swan, "Block Chain: Blueprint for a New Economy", O"Reilly, first edition 2015.
2. Daniel Drescher, "Block Chain Basics", Apress; 1stedition, 2017
3. Anshul Kaushik, "Block Chain and Crypto Currencies", Khanna Publishing House, Delhi.
4. Imran Bashir, "Mastering Block Chain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained", Packt Publishing, first edition – 2012.

Reference Book:

Ritesh Modi, "Solidity Programming Essentials: A Beginner"s Guide to Build Smart Contracts for Ethereum and Block Chain", Packt Publishing.

Websites:

1. https://developer.ibm.com/patterns/create-and-deploy-block chain-network-usingfabric-sdk-java/
2. https://docs.docker.com/get-started/
3. https:/console.ng.bluemix.net/docs/services/block%2520chain/index.html