Indian Institute of Information Technology, Allahabad

Subject Title:*Blockchain & Cryptocurrency*

Course Code: IBCC630E | **IBCC240E** [For B.Tech (IT) and M.Tech (IT)]
LTP credit: L:2 T:1 P:0 | **L:2 T:1 P:1**
Type of Course: Elective

About this course:
Blockchain and Cryptocurrency is vastly discussed now days in all research domains to bring the decentralization. This course is to understand Blockchain and its main application cryptocurrency. Students will learn how this system works and how can they utilize and what application can be build. After successful completion of this course, students will be familiar with blockchain and cryptocurrency concepts. Also they can build their own application using the learned concepts.

Syllabus

- **Basics**: 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.
- **Blockchain**: Introduction, Advantage over conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain.
- **Distributed Consensus**: Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate.
- **Cryptocurrency**: History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Namecoin
- **Cryptocurrency Regulation**: Stakeholders, Roots of Bitcoin, Legal Aspects - Cryptocurrency Exchange, Black Market and Global Economy.
- **Blockchain Applications**: Internet of Things, Medical Record Management System, Domain Name Service and future of Blockchain.

Tutorial & Practical

Naive Blockchain construction, Memory Hard algorithm - Hashcash implementation, Direct Acyclic Graph, Play with Go-ethereum, Smart Contract Construction, Toy application using Blockchain, Mining puzzles

Reference Books and Articles

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
- Wattenhofer, The Science of the Blockchain
- Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
- DR. Gavin Wood, "ETHEREUM: A Secure Decentralized Transaction Ledger,"Yellow paper.2014.
- Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, A survey of attacks on Ethereum smart contracts