# 20IT41E2 - BLOCK CHAIN TECHNOLOGIES

|  |  |  |  |
| --- | --- | --- | --- |
| Course Category: | Professional Elective | Credits: | 3 |
| Course Type: | Theory | Lecture-Tutorial-Practical: | 3-0-0 |
| Prerequisite: | Knowledge in security mechanisms. | Sessional Evaluation:  Univ. Exam Evaluation:  Total Marks: | 40  60  100 |
| Objectives: | * To understand the mechanism of Blockchain and Cryptocurrency. * To understand the functionality of current implementation of blockchain technology. * To understand the required cryptographic background. * To explore the applications of Blockchain to cryptocurrencies and understanding imitations of current Blockchain. | | |

|  |  |  |
| --- | --- | --- |
| Course Outcomes | Upon successful completion of the course, the students will be able to: | |
| CO1 | Understand and apply the fundamentals of Cryptography in Cryptocurrency. |
| CO2 | Acquire knowledge about various operations associated with the life cycle of Blockchain and Cryptocurrency. |
| CO3 | Deal with the methods for verification and validation of Bitcoin transactions. |
| CO4 | Demonstrate the Bitcoin mining of several strategies. |
| CO5 | Understand the methods of Anonymity, Mixing and Decentralized Mixing. |
| CO6 | Awareness the principles, practices and policies associated Bitcoin business. |
| Course Content | UNIT-I  **Introduction to Cryptography and Cryptocurrencies**: Cryptographic Hash Functions, Hash Pointers and Data Structures, Digital Signatures, Public Keys as Identities, A Simple Cryptocurrency.  UNIT-II  **Blockchain Achieves and Store and Use:** Decentralization-Centralization vs. Decentralization-Distributed consensus, Consensus with- out identity using a blockchain, Incentives and proof of work. Simple Local Storage, Hot and Cold Storage, Splitting and Sharing Keys, Online Wallets and Exchanges, Payment Services, Transaction Fees, Currency Exchange Markets.  UNIT-III  **Mechanics of Bitcoin:** Bitcoin transactions, Bitcoin Scripts, Applications of Bitcoin scripts, Bitcoin blocks, The Bit- coin network, Limitations and improvements.  UNIT-IV  **Bitcoin Mining:** The task of Bitcoin miners, Mining Hardware, Energy consumption and ecology, Mining pools, Mining incentives and strategies.  UNIT-V  **Bitcoin and Anonymity:** Anonymity Basics, How to De-anonymize Bitcoin, Mixing, Decentralized Mixing, Zerocoin and Zerocash.  UNIT-VI  **Community, Politics, and Regulation:** Consensus in Bitcoin, Bitcoin Core Software, Stakeholders: Who‟s in Charge, Roots of Bitcoin, Governments Notice on Bitcoin, Anti Money Laundering Regulation, New York‟s Bit License Proposal. Bitcoin as a Platform: Bitcoin as an Append only Log, Bitcoins as Smart Property, Secure Multi Party Lotteries in Bitcoin, Bitcoin as Public Randomness, Source-Prediction Markets, and Real World Data Feeds. | |
| Text Books &  Reference  Books | **TEXT BOOKS:**   1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press 2016.   **REFERENCE BOOKS:**   1. Antonopoulos, A. M. Mastering Bitcoin: unlocking digital cryptocurrencies. O‟Reilly Media, Inc. 2014. 2. Franco, P. Understanding Bitcoin: Cryptography, engineering and economics. John 2014. | |
| E-Resources | 1. <http://nptel.iitm.ac.in> | |