BCSE325L	INTRODUCTION TO BITCOIN	L	T	P	C
		3	0	0	3
Pre-requisite	**NIL**	**Syllabus version**			
		1.0			

Course Objectives

1. To Identify the process of Cryptocurrency.
2. To understand the functionality of Bitcoin.
3. To explore the recent developments on Bitcoin.

Course Outcomes

After completion of this course, the student shall be able to:

1. Understand the fundamentals of Cryptography.
2. Gain knowledge about various operations associated with Cryptocurrency.
3. Develop the methods for verification and validation of Bitcoin transactions.
4. Apply the principles, practices and policies associated with Bitcoin business.

Module:1	**Fundamentals of Cryptography**	**5 hours**

Cryptographic Hash Functions - Hash Pointers and Data Structures - Digital Signatures - Public Keys as Identities - A Simple Cryptocurrency.

Module:2	**Features of Bitcoin**	**6 hours**

Bitcoin Transactions - Bitcoin Scripts - Applications of Bitcoin Scripts - Bitcoin Blocks - Bitcoin Network and Limitations.

Module:3	**Bitcoin Techniques**	**7 hours**

Techniques to Store and Use Bitcoins - Hot and Cold Storage - Splitting and Sharing Keys - Online Wallets and Exchanges - Payment Services - Transaction Fees - Bitcoin Trading.

Module:4	**Bitcoin Mining**	**8 hours**

Task of Bitcoin Miners - Mining Hardware - Energy Consumption and Ecology - Mining Pools - Mining Incentives - Merkley Tree - hardness of mining - transaction verifiability.

Module:5	**Bitcoin and Anonymity**	**5 hours**

Anonymity – Re-identification of Bitcoin - Mixing and Decentralisation of Bitcoin - Zero coin and Zero cash.

Module:6	**Mining Strategies**	**5 hours**

Essential Puzzle Requirements – Application Specific Integrated Circuit Resistant(ASIC) Puzzles - Proof of Volunteer computing - Non externalization of Puzzles - Proof of Stake Virtual Mining.

Module:7	**Bitcoin as a Platform**	**7 hours**

Bitcoin as an Append-Only Log - Bitcoin as Smart Property - Secure Multi-Party Lotteries in Bitcoin - Bitcoin as Randomness Source - Prediction Markets and Real-World Data Feeds.

Module:8	**Contemporary Issues**	**2 hours**
	Total Lecture hours:	**45 hours**

Text Book

1. Goldfeder, S., Bonneau, J., Miller, A., Felten, E., Narayanan, A. Bitcoin and Cryptocurrency Technologies, 2016, 1st edition, Princeton University Press, New Jersey.

Reference Books

1. Antonopoulos, A. M. Mastering Bitcoin: unlocking digital cryptocurrencies, 2017, 2nd edition, OReilly Media, Inc, United States.
2. Lewis, Antony, The Basics Of Bitcoins and Blockchains: An Introduction To Cryptocurrencies and The Technology That Powers Them., 2018, 1st edition, Mango Media Inc., United States.

Mode of Evaluation: CAT / Assignment / Quiz / FAT

Recommended by Board of Studies	04-03-2022		
Approved by Academic Council	No. 65	Date	17-03-2022