Year: B. Tech III (Semester V)

Subject Name: Bitcoin and Cryptocurrencies **Subject Code:** BTEA19526
Type of course: Honors (Group: Blockchain Technology)
Prerequisite (if any): Foundations of Blockchain Technology

Rationale: Bitcoin is a cryptocurrency used to exchange money over internet. An underlying principle behind this course is to teach the students about basics of Bitcoin and its underlying technology. The discussion regarding working with Bitcoin, construction of Bitcoin blockchain and its security is included throughout the course.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
4	0	2	5	60	25	15	30	20	150

CA1: Continuous Assessment (assignments / projects / open book tests / closed book tests) CA2: Sincerity in attending classes / class tests / timely submissions of assignments / self-learning attitude / solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work / Quality of work submitted / Active participation in lab sessions / viva on practical skills learned in course.

Contents:

Sr. No.	Contents	Total Hrs
1.	**Introduction To Bitcoin:** What is Bitcoin, History of Bitcoin, Bitcoin Uses, Users and Their Stories, Getting your first bitcoins, Sending and receiving bitcoins.	06
2.	**Working of bitcoin:** Transactions, Blocks, Mining, and the Blockchain, bitcoin Overview, Bitcoin Transactions, Common Transaction Forms, Constructing a Transaction, Getting the right inputs, Creating the outputs, Adding the transaction to the ledger, Bitcoin Mining, Mining transactions in blocks, Spending the transaction, Bitcoin Client- Bitcoin Core implementation, Running Bitcoin Core for the first time, Compiling Bitcoin Core from the source code, Using Bitcoin Core's JSON-RPC API from the command line.	10
3.	**Bitcoin Key, Addresses, Wallet And Transaction:** Public Key cryptography and generating the public key, Bitcoin addresses and key formats, Bitcoin Wallets and their types, Transaction Lifecycle, Transaction Structure, Transaction Outputs and Inputs, Transaction Scripts and Script Language, Standard Transactions	08
4.	**Bitcoin Network:** Peer-to-Peer Network Architecture, Nodes Types and Roles, The Extended Bitcoin Network, Network Discovery, Full Nodes, Exchanging "Inventory", Simplified Payment Verification (SPV) Nodes, Bloom Filters, Bloom Filters and Inventory Updates, Transaction Pools, Alert Messages	10
5.	**Bitcoin Blockchain:** Structure of a Block, Block Header, Block Identifiers - Block Header Hash and Block Height, The Genesis Block, Linking Blocks in the	12

	Blockchain, Merkle Trees, Merkle Trees and Simplified Payment Verification (SPV), Mining and Consensus. De-centralized Consensus, Independent Verification of Transactions, Mining Nodes, Aggregating Transactions into Blocks, Constructing the Block Header, Mining the Block, Validating a New Block, Consensus Attacks	
6.	**Bitcoin Security And Alternative Currencies:** Security principles, Developing Bitcoin Systems Securely, The Root of Trust, User Security, Physical Bitcoin Storage, Hardware Wallets, Balancing Risk (loss vs. theft), Diversifying Risk, Multi-sig and Governance, Survivability, A taxonomy of alternative currencies and chains, Meta-Coin Platforms, Alt-coins, Non-currency alt-chains	**08**

Suggested Specification table with Marks (Theory): (For B. Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20	20	15	5	-	-

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr No.	Title of book /article	Author(s)	Publisher and details like ISBN
1	Mastering Bitcoin	Andreas M. Antonopoulos	O'Reilly Media, Inc.
2	Bitcoin and crypto currency technologies: a comprehensive introduction	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder.	Princeton University Press

Note: Students should refer to the latest editions of books

Course Outcomes (CO):

Sr. No.	CO statements	Marks % weightage
CO-1	Learn basics of crypto currency and role of Bitcoin in crypto currencies.	30%
CO-2	Create Bitcoin Wallet, Transactions, network and understand their role in implementing Bitcoin BlockChain.	50%
CO-3	Identify key issues of Bitcoin and learn about the alternate crypto currencies.	20%

List of Open learning website:

1. NPTEL: Introduction to Blockchain Technology and Applications (https://nptel.ac.in/courses/106104220)
2. NPTEL: Blockchain Architecture Design And Use Cases (https://nptel.ac.in/courses/106/105/106105184/)
3. Developr's Guide : Bitcoin (https://developer.bitcoin.org/devguide/index.html)

List of Experiments:

Lab Exercises will be based on the theoretical concepts covered in the class

Few sample practical are as follows:

- Visit various BlockChain explorer (blockchain.info, blockexplorer.com, insight.bitpay.com, blockr.io) and study them.
- Study the transaction details on the following url: https://blockchain.info/tx/7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
- Study various command (Words) for Bitcoin scripting language and check their outputs using the following Online Bitcoin Script simulator or debugger
  - https://siminchen.github.io/bitcoinIDE/build/editor.html#
  - https://ide.bitauth.com/
- Write a Bitcoin transaction using the P2PKH script.