Program	Post Graduate Diploma in Data Science
Semester	2
Subject	Blockchain Technology (Elective) (1628005)
Credit	5

Objectives

- To make the students aware about creation of strong cryptographic distributed and replicated ledger of events, transactions, and data generated through various IT processes.
- To make the students familiar with crypto currencies.

Unit No.	Topic(s)	No. of Hours
1.	**Introduction** Basic ideas behind blockchain, How it is changing the landscape of digitalization, Cryptographic basics for cryptocurrency, A short overview of hashing, Signature schemes, Encryption schemes and elliptic curve cryptography	6
2.	**Decentralization and Consensus Algorithms** Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Blockchain and full ecosystem decentralization, Platforms or decentralization, Decentralized web, Decentralized identity, Decentralized finance (DeFi), Introducing the consensus problem, The Byzantine generals problem, Practical Byzantine Fault tolerance (pBFT), Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn (PoB), Proof of Elapsed Time (PoET)	8
3.	**Mechanics of Bitcoin** Bitcoin, Wallet, Blocks, Merkley Tree, Bitcoin transactions, Transaction verifiability, Anonymity, Forks, Double spending, Mathematical analysis of properties of Bitcoin, Bitcoin scripts, Applications of Bitcoin scripts, Bitcoin blocks, The Bitcoin network, Limitations and improvements, How to store and use Bitcoins, Simple local storage, Hot and cold storage, Splitting and sharing keys, Online wallets and exchanges, Payment services, Transaction fees, Currency exchange markets	10
4.	**Alternative coin and Recent Trends** Ethereum, Ethereum Virtual Machine (EVM), Wallets for Ethereum, Solidity, Smart Contracts, some attacks on smart contracts, Zero Knowledge proofs and protocols in Blockchain, Succinct non interactive argument for Knowledge (SNARK), pairing on Elliptic curves, Zcash	8
5.	**Case Studies** Uses of Blockchain in E-Governance, Land Registration, Medical Information Systems and others	8

Reference Books

1. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
   by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder
   Princeton University Press, 2016
2. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrency
   by Joseph Bonneau et al
   IEEE Symposium on Security and Privacy, 2015
3. The bitcoin backbone protocol - analysis and applications
   by J.A.Garay et al
   EUROCRYPT 2015 LNCS VOl 9057, (VOLII), pp 281-310

4. Analysis of Blockchain protocol in Asynchronous networks
   by R.Pass et al
   EUROCRYPT 2017, (eprint.iacr.org/2016/454), A significant progress and consolidation of several principles

Outcomes

After completion of subject, students would be able to:

- familiarise the functional/operational aspects of cryptocurrency.
- understand emerging abstract models for Blockchain Technology.
- identify major research challenges and technical gaps existing between theory and practice in cryptocurrency domain.

Suggested list of Practical (at least 10 practical are to be performed by students. These practical should cover majority of all topics of syllabus.)
This is the suggested list of practical but it may not be limited only to this list.

1. Create different types of Blockchain bitcoin wallet.
2. Do the Bitcoin Transaction from bitcoin wallet.
3. Implement Merkley tree hash algorithm.
4. Set up an environment for Ethereum on Windows and Linux.
5. Install & setup Ethereum wallet and send/receive ether.
6. Create smart contracts using solidity.
7. Create smart contract for connect with the front end (web page).
8. Implement smart contract to send ether to another contract/address.
9. Implement smart contract for deposit and withdrawals money from digital bank.
10. Implement zero knowledge proof protocol using blockchain.