PGDDS 505 Blockchain Technology 3(2+1)

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 I: 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

Unit II: Models for Blockchain: The Consensus problem, Asynchronous Byzantine Agreement, AAP protocol and its analysis, Nakamoto Consensus on permission-less, nameless, peerto- peer network, Abstract Models for Blockchain, GARAY model, RLA Model, Proof of Work (PoW) as random oracle, formal treatment of consistency, liveness and fairness, Proof of Stake (PoS) based Chains, Hybrid models (PoW + PoS)

Unit III: 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

Unit IV: 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

Unit V: Case Studies: Uses of Blockchain in E-Governance, Land Registration, Medical Information Systems and others

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