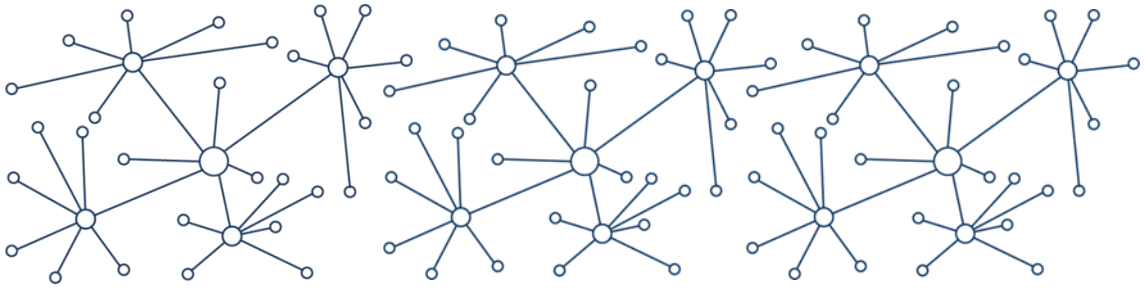

# Blockchain Technology

## Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#1 and 2 (26-27 July 2022)

Dr. Dhiren Patel

# Welcome note

- Digital divide (bandwidth, power, device, platform)
- NEP – New Education Policy
- Capacity building, Re-training, Up-skilling (Deep skilling)
- Personalized Education – Digital way
- As responsible citizens, all of us should fight the pandemic and other hardships, and showcase our capabilities and commitment towards economic progress with social inclusion and environment sustainability for the global good

# What is a Blockchain? Why should we learn it?

- Blockchain facilitates peer-to-peer transfer of *digital assets* in a *decentralized network*
- It is a time-stamped series of (immutable) records of data that is managed by a cluster of nodes (computers) not owned by any single entity (?) - **a democratized system**
- A technology originally created to support *cryptocurrency* bitcoin - Founder (pseudo-named) – **Satoshi Nakamoto**
- Blockchain has the potential to improve applications in finance, healthcare, government, manufacturing, and distribution supply chain…
- There is a dire need for designers, developers, and critical thinkers, who can envision and create newer application models on Blockchain to benefit the world

# Security primitives and its use

- Hash function (cryptographic) – e.g. SHA2
- Encryption (Block cipher, Stream cipher, Symmetric Key Encryption, Public Key Encryption)
- AES, RSA, Elliptic Curve
- Key management and Key exchange (Security Association)
- Example: Banking – end-of-day reconciliation

# Blockchain

- Think of blockchain as a historical fabric underneath recording everything that happens—every digital transaction; exchange of value, goods and services; or private data—exactly as it occurs.
- Then the chain stitches that data into (encrypted??) blocks that can never be modified and scatters the pieces across a worldwide network of distributed computers or "nodes.“
- A blockchain is made up of two primary components: a decentralized network facilitating and verifying transactions, and the immutable ledger that network maintains.
- Welcome aboard in the World of Blockchain!!

# Know the Course CS423

- Course scheme (3-0-0) – Core Elective 3 <see next slide>
- Course Objectives, Outcome and Curriculum/Syllabus
- Teaching methodology (Interactions and Hands on)
- Book(s), Reference(s), PPTs, Papers (ACM, IEEE, etc..), MooCs
- Course repository – Google classroom (**Class code: 3wcypqj**)
- Evaluation - **Relative Grading (Open Notes?)**
- **Mid-sem, End-sem, Assignments (coding/math/design), Quizzes/Tests, Attendance requirement (?)**

# Teaching Scheme of B.Tech.-IV (CSE) (Semester VII)

| Sr. No. | Course | Code | Credit | Teaching Scheme | | | Examination Scheme | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | L | T | P | L | T | P | |
| 1 | Software Engineering (Core-15) | CS401 | 5 | 3 | 1 | 2 | 100 | 25 | 50 | 175 |
| 2 | Innovation, Incubation and Entrepreneurship | HU410 | 3 | 3 | 0 | 0 | 100 | 0 | 0 | 100 |
| 3 | Core Elective-3 | CS4AA | 3 | 3 | 0 | 0 | 100 | 0 | 0 | 100 |
| 4 | Core Elective-4 | CS4BB | 3 | 3 | 0 | 0 | 100 | 0 | 0 | 100 |
| 5 | Summer Training* | CS403 | 2 | 0 | 0 | 0 | 0 | 0 | 50 | 50 |
| 6 | Project Preliminaries | CS405 | 3 | 0 | 0 | 6 | 0 | 0 | 150 | 150 |
| | **Total** | | **19** | **12** | **1** | **8** | **400** | **25** | **250** | **675** |
| | **Total Contact Hours per week** | | | **21** | | | | | | |

**Core Elective-3 (CS4AA):**

| | | | |
|---|---|---|---|
| 1 | Computer Graphics (CS421) | 4 | Video Codec standards and Design (CS427) |
| 2 | Blockchain Technology (CS423) | 5 | Computational Geometry (CS429) |
| 3 | Smartphone Computing and Applications (CS425) | | |

**B.Tech. IV (CSE) Semester – VII**
**BLOCKCHAIN TECHNOLOGY (CORE ELECTIVE - 3)**
**CS423**

| | L | T | P | Credit |
|---|---|---|---|---|
| **Scheme** | **3** | **0** | **0** | **03** |

---

**1. Course Outcomes (COs):**

**At the end of the course, students will be able to**

| | |
|---|---|
| CO1 | understand the need, functions and challenges of blockchain technology. |
| CO2 | deploy smart contracts for given use cases. |
| CO3 | analyse blockchain based system structure and security offered therein. |
| CO4 | asses functions, benefits and limitations of various blockchain platforms. |
| CO5 | design and develop solution using blockchain technology in various application domains. |

# Syllabus

- **INTRODUCTION** **(04 Hours)**

  Introduction to Blockchain Technology, Concept of Blocks, Transactions, Distributed Consensus, the Chain and the Longest Chain, Cryptocurrency, Blockchain 2.0, Permissioned Model of Blockchain, Permission less Blockchain.

- **DECENTRALIZATION USING BLOCKCHAIN** **(06 Hours)**

  Methods of Decentralization, Disintermediation, Contest-Driven Decentralization, Routes to Decentralization, the Decentralization Framework Example, Blockchain and Full Ecosystem Decentralization, Storage, Communication, Computing Power and Decentralization, Smart Contracts, Decentralized Autonomous Organizations, Decentralized Applications (DApps), Requirements and Operations of DApps, DApps Examples, Platforms for Decentralizations.

- **CRYPTO PRIMITIVES FOR BLOCKCHAIN** **(04 Hours)**

  Symmetric and Public Key Cryptography, Cryptographic Hard Problems, Key Generation, Secure Hash Algorithms, Hash Pointers, Digital Signatures, Merkle Trees, Patricia trees, Distributed Hash Tables.

# Syllabus - cont

- **BITCOINS AND CRYPTOCURRENCY** **(06 Hours)**

  Introduction, Digital Keys and Addresses, Private and Public Keys in Bitcoins, Base58Check Encoding, Vanity Addresses, Multi Signature Addresses, Transaction Lifecycle, Data Structure for Transaction, Types of Transactions, Transaction Verification, The Structure of Block in Blockchain, Mining, Proof of Work, Bitcoin Network and Payments, Bitcoin Clients and APIs, Wallets, Alternative Coins, Proof of Stake, Proof of Storage, Various Stake Types, Difficulty Adjustment and Retargeting Algorithms, Bitcoin Limitations.

- **SMART CONTRACTS** **(02 Hours)**

  Smart Contract Templates, Oracle, Smart Oracle, Deploying Smart Contract on Blockchain.

- **PERMISSIONED BLOCKCHAIN** **(05 Hours)**

  Models and Use-cases, Design Issues, Consensus, Paxos, RAFT Consensus, Byzantine General Problem, Practical Byzantine Fault Tolerance.

# Syllabus - cont

- **DEVELOPMENT TOOLS AND FRAMEWORKS** **(05 Hours)**

  Solidity Compilers, IDEs, Ganache, Metamask, Truffle, Contract Development and Deployment, Solidity Language, Types, Value Types, Literals, Enums, Function Types, Reference Types, Global Variables, Control Structures, Layout of Solidity Source Code File.

- **HYPERLEDGER** **(05 Hours)**

  The Reference Architecture, Requirements and Design Goals of Hyperledger Fabric, The Modular Approach, Privacy and Confidentiality, Scalability, Deterministic Transactions, Identity, Auditability, Interoperability, Portability, Membership Services in Fabric, Blockchain Services, Consensus Services, Distributed Ledger, Sawtooth Lake, Corda.

- **BLCOKCHAIN USE-CASES AND CHALLENGES** **(05 Hours)**

  Finances, Government, Supply Chain, Security, Internet of Things, Scalability and Challenges, Network Plane, Consensus Plane, Storage Plane, View Plane, Block Size Increase, Block Interval Reduction, Invertible Bloom Lookup Tables, Private Chains, Sidechains, Privacy Issues, Indistinguishability Obfuscation, Homomorphic Encryption, Zero Knowledge Proofs, State Channels, Secure Multiparty Computation, Confidential Transactions.

**(Total Contact Time = 42 Hours)**

# Course objectives

- Capacity building - Learning through examples/use cases
- Understand technology foundations of Blockchain through protocols, security primitives, token economics, smart contracts, attacks and advances
- Design and implement new ways of using blockchain for applications with cryptocurrency and beyond
- Explore platforms to build applications on blockchain

# Course outcome ()

1. Understand blockchain architecture and requisite crypto foundations
2. Understand various consensus protocols and their usage for specific applications
3. Understand and Resolve security concerns in blockchain
4. Explore blockchain advances, use cases and upcoming platforms
5. Learn to write smart contracts
6. Solve problems and create solutions..

# Instructor(s)

- Disciplines/Departments/Compartments?? (**NEP**)
- Boundary-less, Flexible, Autonomous education ecosystem
- Instructors (Fall 2022) –
  - Dr Dhiren Patel (2 hrs/week)
  - Himanshu (TA) (1 hr/week)
  - Visiting faculty (on-line/on-campus)
  - Dr Mahesh Shirole (VJTI Mumbai)
  - Dr Yann Busnel (IMT Atlantique Rennes France),
  - Jay Bothra (HSBC London)
  - Mugdha Bhagwat (Morgan Stanley)
  - Sanket Shah (VJTI Mumbai), …. And more

**Thank you**

**for your attention**