A TEXT BOOK OF

BLOCKCHAIN TECHNOLOGY

(Elective - III)

FOR
SEMESTER – VII

FINAL YEAR B. TECH. COURSE IN
ARTIFICIAL INTELLIGENCE & DATA SCIENCE /
ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

Strictly According to New Revised Credit System Syllabus of
Dr. Babasaheb Ambedkar Technological University (DBATU),
Lonere, (Dist. Raigad) Maharashtra.
(w.e.f. 2023-24)

Dr. NITIN N. SAKHARE
Ph.D. (CSE)
Assistant Professor,
Dept. of Computer Engg.,
Vishwakarma Institute of Information Technology,
Pune.

Dr. RADHIKA G. PURANDARE
Ph.D. (E&TC)
Associate Professor,
Dept. of E&TC Engg.,
Vishwakarma Institute of Information Technology,
Pune.

DHARMESH DHABLIYA
Doctorate in Business Administration (Switzerland)
Assistant Professor,
Dept. of Information Technology,
Vishwakarma Institute of Information Technology,
Pune.

Dr. SHARDDHA R. KHONDE
Ph.D. (Computer Engg.)
Assistant Professor,
Dept. of Computer Engg.,
Modern Education Society's Wadia College of Engg.,
Pune.

Price ₹ 170.00

NIRALI PRAKASHAN
ADVANCEMENT OF KNOWLEDGE

N3009

BLOCKCHAIN TECHNOLOGY (DBATU) **ISBN : 978-93-6109-977-9**

First Edition : March 2024
© : Authors

The text of this publication, or any part thereof, should not be reproduced or transmitted in any form or stored in any computer storage system or device for distribution including photocopy, recording, taping or information retrieval system or reproduced on any disc, tape, perforated media or other information storage device etc., without the written permission of Authors with whom the rights are reserved. Breach of this condition is liable for legal action.

Every effort has been made to avoid errors or omissions in this publication. In spite of this, errors may have crept in. Any mistake, error or discrepancy so noted and shall be brought to our notice shall be taken care of in the next edition. It is notified that neither the publisher nor the authors or seller shall be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom. The reader must cross check all the facts and contents with original Government notification or publications.

Published By :
NIRALI PRAKASHAN
Abhyudaya Pragati, 1312 Shivaji Nagar
Off J.M. Road, PUNE 411005
Tel : (020) 25512336/37/39
Email : niralipune@pragationline.com

Polyplate

Printed By :
YOGIRAJ PRINTERS AND BINDERS
Survey No. 10/1A, Ghule Industrial Estate
Nanded Gaon Road
Nanded, Pune 411041

DISTRIBUTION CENTRES

PUNE

Nirali Prakashan
(For orders outside Pune)
S. No. 28/27, Dhayari Narhe Road, Near Asian College
Pune 411041, Maharashtra
Tel : (020) 24690204; Mobile : 9657703143
Email : bookorder@pragationline.com

Nirali Prakashan
(For orders within Pune)
119, Budhwar Peth, Jogeshwari Mandir Lane
Pune 411002, Maharashtra
Mobile : 9657703145, 9890997937
Email : niralilocal@pragationline.com

MUMBAI

Nirali Prakashan
Rasdhara Co-op. Hsg. Society Ltd., 'D' Wing Ground Floor, 385 S.V.P. Road
Girgaum, Mumbai 400004, Maharashtra
Mobile : 7045821020, Tel : (022) 2385 6339 / 2386 9976
Email : niralimumbai@pragationline.com

DISTRIBUTION BRANCHES

DELHI

Nirali Prakashan
Room No. 2 Ground Floor
4575/15 Omkar Tower, Agarwal Road
Darya Ganj, New Delhi 110002
Mobile : 9555778814/9818561840
Email : delhi@niralibooks.com

BENGALURU

Nirali Prakashan
Maitri Ground Floor, Jaya Apartments, No. 99, 6th Cross, 6th Main, Malleswaram, Bengaluru 560003 Karnataka; Mob : 9686821074
Email : bengaluru@niralibooks.com

NAGPUR

Nirali Prakashan
Above Maratha Mandir, Shop No. 3, First Floor, Rani Jhanshi Square, Sitabuldi Nagpur 440012 (MAH)
Tel : (0712) 254 7129
Email : nagpur@niralibooks.com

KOLHAPUR

Nirali Prakashan
438/2, Bhosale Plaza, Ground Floor, Khasbag, Opp. Balgopal Talim, Kolhapur 416 012 Maharashtra
Mob : 9850046155
Email : kolhapur@niralibooks.com

JALGAON

Nirali Prakashan
34, V. V. Golani Market, Navi Peth, Jalgaon 425001, Maharashtra
Tel : (0257) 222 0395
Mob : 94234 91860
Email : jalgaon@niralibooks.com

SOLAPUR

Nirali Prakashan
R-158/2, Avanti Nagar, Near Golden Gate, Pune Naka Chowk
Solapur 413001, Maharashtra
Mobile 9890918687
Email : solapur@niralibooks.com

PREFACE

It gives us great pleasure to present the book **"Blockchain Technology" (Elective - III)** for the students of **Semester VII Final Year B. Tech. Course in Artificial Intelligence & Data Science / Artificial Intelligence & Machine Learning of Dr. Babasaheb Ambedkar Technological University (DBATU), Lonere, Dist. Raigad (Maharashtra)**. This book is strictly as per the new revised syllabus 2020 Pattern, effective from the Academic Year July 2023-24.

In New Revised Syllabus, there will be Internal Assessment (20 Marks), Mid Sem. Exam. (20 Marks) and End Sem. Exam. (60 Marks). End Sem. Exam. will be based on all Five units.

The Theory Course will have 4 Credits.

The basic objective of this book is to bridge the gap between the vast contents of the reference books, written by renowned International Authors and the concise requirements of Undergraduate Students. This book has been written in a comprehensive manner using Simple and Lucid language, keeping in mind students' requirements. The main emphasis has been given on exploring the basic concepts rather than merely the Information. Solved Examples and Exercises have been provided throughout the book and at the end of the Unit. Also, we have given **Model Question Papers** for practice at the end of book.

We also take this opportunity to express our sincere thanks to Shri. Dineshbhai Furia, Shri. Jignesh Furia, Mrs. Nirali Verma and entire team of Nirali Prakashan, namely Mrs. Deepali Lachake (Co-ordinator), who really have taken keen interest and untiring efforts in publishing this text.

We wish to make a special mention of the valuable contribution made by Late Shri M.P. Munde during the last two decades in reaching out to students, parents and teachers which eventually made **Nirali Prakashan, a brand of trust and quality in technical books.** Without his perseverance and zeal, successive editions would not have been possible.

Suggestions of our esteemed readers are most welcome and will be highly appreciated.

Pune **Authors**

SYLLABUS

Unit I: Introduction to Blockchain **[7 Hours]**

History of blockchain, Peer-to-Peer (P2P) network, public ledger, double spend problem, features of blockchain, types of blockchain: public, private and consortium based blockchain and applications of blockchain.

Unit II: Cryptographic Primitives **[7 Hours]**

Public key cryptography, hash functions, message digest, secure hash algorithms (SHAS- 256), digital signature, elliptic curve digital signature algorithms (ECDSA), merkle tree.

Unit III: Bitcoin Definition, Transactions **[8 Hours]**

The transaction life cycle, the structure of a block, genesis block, wallet, bitcoin mining, forking: hard and soft fork. Consensus algorithms: proof of work, proof of stake, practical byzantine fault tolerance, proof of burn and prof of elapsed time.

Unit IV: Smart Contracts, Ethereum Basics **[7 Hours]**

Introduction to Ethereum & Ether, Gas, the world state, transactions, Ethereum virtual machine (EVM), types of accounts, block structure, ether, DApps. Ethereum vs bitcoin.

Unit V: Blockchain Use Cases **[7 Hours]**

Land Registry Records, Cross-border payments over blockchain, Project Ubin, Food Security, Supply chain financing, Voting system and Identity on Blockchain, Supply chain management, Healthcare and electronic medical records, Blockchain and Metaverse.

CONTENTS

Unit I: Introduction to Blockchain **1.1-1.20**

1.1 History of Blockchain 1.1
- 1.1.1 What is Blockchain? 1.1
- 1.1.2 Blockchain Historical Building Blocks 1.1
- 1.1.3 Working of Blockchain 1.2

1.2 Peer-to-Peer (P2P) Network 1.6
- 1.2.1 History of P2P Networks 1.6
- 1.2.2 Type of P2P Networks 1.6
- 1.2.3 Features of P2P Network 1.6
- 1.2.4 Architecture of P2P Network 1.7
- 1.2.5 Working of P2P Network 1.7
- 1.2.6 Applications of P2P Network 1.7

1.3 Public Ledger 1.9
- 1.3.1 Elements of Public Ledger 1.9
- 1.3.2 Working of Cryptocurrency Public Ledgers 1.9

1.4 Double Spend Problem 1.10
- 1.4.1 What is Double Spending? 1.10
- 1.4.2 Types of Double Spending Attacks 1.11
- 1.4.3 Solutions to Prevent Double Spending 1.12

1.5 Features of Blockchain 1.13

1.6 Types of Blockchain 1.15
- 1.6.1 Public Blockchain 1.15
- 1.6.2 Private Blockchain 1.15
- 1.6.3 Consortium Based Blockchain 1.16
- 1.6.4 Features of Consortium Blockchain 1.16

1.7 Applications of Blockchain 1.18

- **Exercise** 1.19

Unit II: Cryptographic Primitives **2.1-2.26**

2.1 Public Key Cryptography 2.1
- 2.1.1 Encryption 2.1
- 2.1.2 Decryption 2.1
- 2.1.3 Weakness of the Public Key Encryption 2.2
- 2.1.4 What is Asymmetric Cryptography? 2.2
- 2.1.5 Uses of Asymmetric Cryptography 2.3
- 2.1.6 What are the Advantages and Disadvantages of Asymmetric Cryptography? 2.3
- 2.1.7 What's the Difference Between Asymmetric vs. Symmetric Cryptography? 2.4
- 2.1.8 What are Examples of Asymmetric Cryptography? 2.4
- 2.1.9 What's the History of Asymmetric Cryptography? 2.4

2.2 Hash Functions 2.5
2.2.1 Features of Hash Functions 2.5
2.2.2 Properties of Hash Functions 2.5
2.2.3 Design of Hashing Algorithms 2.5
2.2.4 Popular Hash Functions 2.6
2.2.5 Applications of Hash Functions 2.7
2.3 Message Digest 2.7
2.3.1 What is MD5? 2.8
2.3.2 What is MD5 Used for? 2.8
2.3.3 Message-Digest Algorithm Characteristics 2.8
2.3.4 How Does MD5 Work? 2.9
2.3.5 Is MD5 Secure? 2.9
2.3.6 Alternatives to MD5 2.9
2.4 Secure Hash Algorithms (SHAS- 256) 2.9
2.4.1 SHA Introduction 2.9
2.4.2 Different Types of SHA 2.10
2.4.3 Why and How SHA is Used? 2.10
2.4.4 The Prospects for Hashing 2.11
2.4.5 What is Hashing? 2.11
2.4.6 What is the SHA-256 Algorithm? 2.11
2.4.7 What are the Characteristics of the SHA-256 Algorithm? 2.11
2.4.8 Steps in SHA-256 Algorithm 2.12
2.4.9 Padding Length 2.12
2.4.10 A Definitive Guide to Learn the SHA-256 (Secure Hash Algorithms) 2.12
2.4.11 Initialising the Buffers 2.12
2.4.12 Compression Functions 2.13
2.4.13 Output 2.13
2.5 Digital Signature 2.13
2.5.1 What is a Digital Signature? 2.13
2.5.2 How do Digital Signatures Work? 2.13
2.5.3 What are the Advantages of Digital Signatures? 2.14
2.5.4 How do you Create a Digital Signature? 2.14
2.5.5 Classes and Types of Digital Signatures 2.15
2.5.6 Uses for Digital Signatures 2.15
2.5.7 Why Use PKI or PGP with Digital Signatures? 2.16
2.5.8 What's the Difference Between a Digital Signature and an Electronic Signature? 2.16
2.5.9 Digital Signature Security 2.17
2.5.10 Digital Signature Attacks 2.17
2.5.11 Digital Signature Tools and Vendors 2.17

2.6 Elliptic Curve Digital Signature Algorithms (ECDSA) 2.17
2.6.1 What is ECDSA? 2.18
2.6.2 Digital Signature of ECDSA 2.18
2.6.3 Domain Parameter of ECDSA 2.18
2.6.4 Domain Parameter Validation 2.19
2.6.5 ECDSA Key Pair 2.19
2.7 Merkle Tree 2.24
2.7.1 What is a Merkle Tree? 2.24
2.7.2 What is a Merkle Root? 2.24
2.7.3 Cryptographic Hash Functions 2.24
2.7.4 Working of Merkle Trees 2.24
2.7.5 Why is it Essential to Blockchain? 2.25
2.7.6 Use-Cases of Merkle Tree in Blockchain 2.26
- **Exercise** 2.26

Unit III: Bitcoin Definition, Transactions 3.1-3.26

3.1 The Transaction Life Cycle 3.1
3.1.1 Deloitte 3.2
3.1.2 Wall Street Analyst 3.3
3.1.3 i-Scoop and Accenture 3.4
3.1.4 Zero Hedge 3.5
3.2 The Structure of a Block 3.7
3.3 Genesis Block 3.7
3.3.1 Features of Genesis Block 3.7
3.3.2 Why Genesis Block is Needed? 3.8
3.3.3 How to Verify Genesis Block? 3.8
3.3.4 Significance of Genesis Block 3.9
3.4 Wallet 3.9
3.4.1 Features of Blockchain Wallet 3.9
3.4.2 Types of Blockchain Wallets 3.10
3.4.3 Criteria to Choose Blockchain Wallet 3.11
3.5 Bitcoin Mining 3.12
3.5.1 What is Bitcoin Mining? 3.12
3.5.2 How Does Bitcoin Mining Work? 3.12
3.5.3 How Blockchian Works 3.13
3.5.4 The Economics of Bitcoin Mining 3.14
3.5.5 The History of Bitcoin Mining 3.15
3.6 Forking 3.15
3.6.1 Types of Forks 3.16
3.6.2 Future of the Blockchain Fork 3.16
3.6.3 Hard Fork 3.17
3.6.4 Soft Fork 3.17

3.7 Consensus Algorithms 3.17
3.7.1 Proof of Work 3.17
3.7.2 Proof of Stake 3.19
3.7.3 Practical Byzantine Fault Tolerance 3.20
3.7.4 Proof of Burn 3.22
3.7.5 Proof of Elapsed Time 3.23
- **Exercise** 3.25

Unit IV: Smart Contracts, Ethereum Basics 4.1-4.20

4.1 Introduction to Ethereum 4.1
4.1.1 What is Ethereum? 4.1
4.1.2 History of Ethereum 4.1
4.1.3 Features of Ethereum 4.1
4.1.4 Type of Ethereum Accounts 4.2
4.1.5 Working of Ethereum 4.2
4.1.6 Applications of Ethereum 4.2
4.2 Ether 4.3
4.2.1 What is Ether? 4.3
4.2.2 Uses of Ether 4.3
4.3 Gas 4.4
4.3.1 Gas Limit 4.4
4.3.2 Gas Price 4.4
4.4 Ethereum World State 4.4
4.4.1 Various States and Working of Ethereum 4.5
4.4.2 Types of Account's in World State 4.6
4.5 Transactions in Ethereum 4.7
4.5.1 Components of Transaction 4.7
4.6 Ethereum Virtual Machine (EVM) 4.8
4.6.1 Explanation of Ethereum Virtual Machine (EVM) 4.8
4.6.2 Features of the Ethereum Virtual Machine (EVM) 4.9
4.6.3 What Powers the Ethereum Virtual Machine? 4.10
4.6.4 Explanation EVM through Orderly Network 4.10
4.7 Types of Accounts 4.10
4.7.1 What are Ethereum Accounts? 4.10
4.7.2 Types of Ethereum Accounts 4.11
4.7.3 Types of Contract Accounts 4.11
4.7.4 Different Fields in Ethereum Accounts 4.11
4.8 Block Structure in Ethereum 4.12
4.8.1 What is Block in Ethereum? 4.12
4.8.2 Structure of Blocks 4.13

4.9 DApps 4.17
4.9.1 Working of DApps 4.17
4.9.2 Scams in DApp 4.18
4.9.3 Comparing Centralized vs. Decentralized Apps 4.18
4.10 Ethereum vs. Bitcoin 4.19
4.10.1 Introduction to Ethereum and Bitcoin 4.19
4.10.2 Differences between Ethereum and Bitcoin 4.19
- **Exercise** 4.20

Unit V: Blockchain Use Cases **5.1-5.20**

5.1 Land Registry Records 5.1
5.1.1 A Failing System 5.2
5.1.2 Putting Land Registries on the Blockchain 5.4
5.1.3 From Centralization to Decentralization 5.4
5.1.4 Trust and Transactions 5.5
5.1.5 Land Registration – Certification Issuance, Title Transfer and Taxation 5.6
5.2 Cross-Border Payments Over Blockchain 5.9
5.3 Project Ubin 5.10
5.4 Food Security 5.11
5.5 Supply Chain Financing 5.12
5.6 Voting System and Identity on Blockchain 5.13
5.7 Supply Chain Management 5.14
5.8 Healthcare and Electronic Medical Records 5.15
5.9 Blockchain and Metaverse 5.16
- **Exercise** 5.20

- **Model Question Papers for**
  - ➢ **Mid-Semester Examination (20 Marks)** **P.1-P.1**
  - ➢ **End-Semester Examination (60 Marks)** **P.2-P.2**

✠ ✠ ✠

UNIT - I

INTRODUCTION TO BLOCKCHAIN

1.1 HISTORY OF BLOCKCHAIN

Blockchain was officially introduced in 2009 with the release of its first application the Bitcoin cryptocurrency but its roots reach back several decades. Many of the technologies that form the basis for blockchain today were in the works long before the emergence of Bitcoin.

Still, blockchain most identifies with Bitcoin for better or worse. In the wild and raucous years that followed Bitcoin's debut, blockchain earned a reputation akin to the Wild West. Its decentralized, Peer-to-Peer (P2P) architecture allowed just about anyone to participate in the process, making it seem too risky for business use. That started to change in 2016 when a burgeoning open source community began developing complete enterprise platforms.

Since then, the technology has taken on a life of its own, with interest coming from many quarters, despite the sometimes scary cryptocurrency headlines of late. Governments, businesses and other organizations are researching and deploying blockchain technology to meet needs that have nothing to do with digital currency. In the face of proliferating cyberthreats and government data privacy regulations, blockchain offers security, immutability, traceability and transparency across a distributed network, making it well suited for use cases that have become difficult to support and protect with traditional infrastructures.

1.1.1 What is Blockchain?

Blockchain is a type of database that's a public ledger for recording transactions without the need for a third party to validate each activity. It's distributed across a P2P network and consists of data blocks linked together to form a continuous chain of immutable records. Each computer in the network maintains a copy of the ledger to avoid a single point of failure. Blocks are added in sequential order, and they're permanent and tamperproof.

A blockchain starts with an initial block often referred to as the Genesis block that records the first transactions. The block is also assigned an alphanumeric string called a hash, which is based on the block's timestamp. Blocks are added to the chain sequentially. Each block uses the hash from the previous block to create its own hash, thus linking the blocks together.

Blockchain also uses a computational process called consensus to validate a block's authenticity before it can be added to the chain. As part of this process, most of the nodes on the blockchain network must agree that the new block's hash has been calculated correctly. Consensus ensures that all copies of the distributed ledger are in the same state.

Initially, blockchain provided a distributed public ledger to support Bitcoin, so transactions could be recorded without the need for a central authority to establish trust in a trustless environment. Not only were transactions more efficient, but also the costs typically associated with third-party verification were eliminated. Blockchain also provided greater transparency, traceability and security than conventional approaches to handling distributed transactions.

1.1.2 Blockchain Historical Building Blocks

Although blockchain as an entity has a relatively short history, its influence today is widespread and its applications wide-ranging and growing. Through the decades, blockchain's development and evolution include some of the following notable developments:

- Pioneers like Merkle and his tree, Chaum and digital cash, Haber and timestamping, Dwork and Proof of Work (PoW), Black and hashcash, Finney and reusable PoW dotted the early years of the pre-blockchain landscape.
- The presumed pseudonym Satoshi Nakamoto was created to introduce the concept of cryptocurrency and blockchain. Shortly thereafter, cryptocurrency was launched and Nakamoto conducted the first bitcoin transaction, a bitcoin exchange was established and a programmer paid 10,000 bitcoin for two pizzas.
- Bitcoin's price soared from pennies to tens of thousands of dollars, all the while draped in controversies, shutdowns, crackdowns, bankruptcies, scams, scandals and arrests.

- Blockchain started to somewhat divorce itself from Bitcoin when the decentralized blockchain platform Ethereum eventually became one of the biggest applications of blockchain technology and opened the door to numerous business applications beyond cryptocurrencies.
- And buoyed by AI, IoT, Non-Fungible Tokens (NFTs), Decentralized Finance (DeFi) and smart contracts, as well as initiatives by the likes of Walmart and Amazon, blockchain has gained legitimacy as a safe, viable alternative to traditional methods of conducting business and individual transactions.

1.1.3 Working of Blockchain

1. Transaction
2. Block
3. Verification
4. Hash
5. Execution

1. Transaction: Two parties, A and B, decide to exchange a unit of value (digital currency or a digital representation of some other asset, such as land title, birth certificate or educational degree) and initiate the transaction.

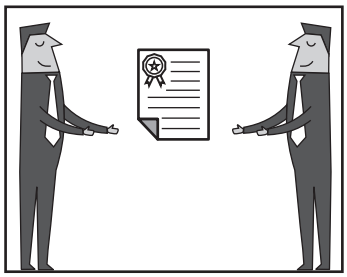


Fig. 1.1

2. Block: The transaction is packed with other pending transactions thereby created a "block". The block is sent to the blockchain system's network of participating computers.

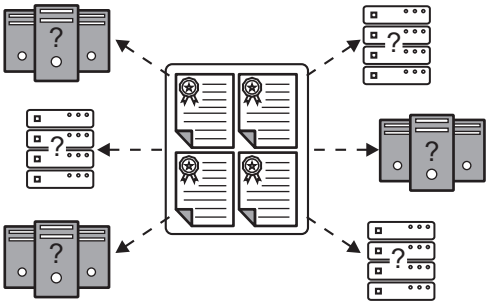


Fig. 1.2

3. Verification: The participating computers (called "miners" in the Bitcoin blockchain) evaluate the transactions and through mathematical calculations determine whether they are valid, based on agreed-upon rules. When "consensus" has been achieved, typically among 51% of participating computer's the transactions are considered verified.

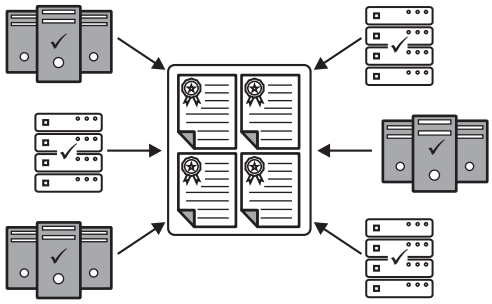


Fig. 1.3

4. Hash: Each verified block of transactions is time-stamped with a cryptographic hash. Each block also contains a reference to the previous block's hash, thus creating a "chain" of records that cannot be falsified except by convincing participating computers that the tampered data in one block and in all prior blocks is true. Such a feat is considered impossoble.

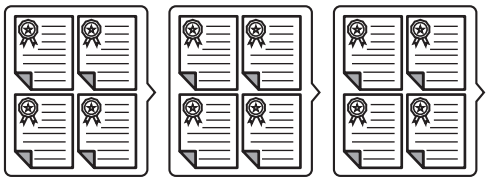


Fig. 1.4

5. Execution: The unit of value moves from the account of party A to the account of party B.

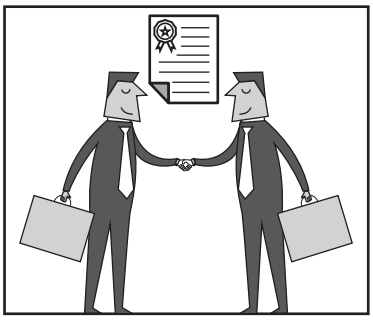


Fig. 1.5

- **1979:** One of the early pre-blockchain technologies is the Merkle tree, named after computer scientist and mathematician Ralph Merkle. He described an approach to public key distribution and digital signatures called tree authentication in his Ph.D. thesis for Stanford University. Merkle eventually patented this