



Blockchain Essentials

Core Concepts and Implementations

Ramchandra Sharad Mangrulkar
Pallavi Vijay Chavan

Apress®

Blockchain Essentials

Ramchandra Sharad Mangrulkar • Pallavi Vijay Chavan

Blockchain Essentials

Core Concepts and Implementations

Apress®

Ramchandra Sharad Mangrulkar
Mumbai, Maharashtra, India

Pallavi Vijay Chavan
Mumbai, Maharashtra, India

ISBN-13 (pbk): 978-1-4842-9974-6

ISBN-13 (electronic): 978-1-4842-9975-3

<https://doi.org/10.1007/978-1-4842-9975-3>

Copyright © 2024 by Ramchandra Sharad Mangrulkar and Pallavi Vijay Chavan

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr

Acquisitions Editor: Smriti Srivastava

Development Editor: Laura Berendson

Coordinating Editor: Shaul Elson

Cover designed by eStudioCalamar

Cover image by Sketchepedia@freepik.com

Distributed to the book trade worldwide by Apress Media, LLC, 1 New York Plaza, New York, NY 10004, U.S.A. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub (<https://github.com/Apress>). For more detailed information, please visit <https://www.apress.com/gp/services/source-code>.

Paper in this product is recyclable

*To our cherished daughter, Mansi:
Your unwavering support, encouragement, and constant
sympathy were invaluable during the creation of this book.
Without you, it would have been completed in half the time.*

Contents

1	Introduction to Blockchain	1
1.1	Prerequisites	1
1.2	Blockchain Myths	2
1.3	Blockchain and Decentralization	2
1.4	What Is Blockchain?	3
1.5	Disruptive Technology	4
1.6	History	5
1.6.1	Milestones in Blockchain Development	5
1.7	Features of Blockchain	7
1.8	Present Growth	9
1.9	Predicted Market	9
1.10	Blockchain Types	10
1.10.1	Public	11
1.10.2	Private	12
1.10.3	Federated	12
1.10.4	Hybrid	13
1.10.5	Difference Between Public and Private Blockchains	14
1.11	Blockchain Framework	14
1.11.1	Hardware/Infrastructure Layer	14
1.11.2	Data Layer	15
1.11.3	Network Layer	16
1.11.4	Consensus Layer	16
1.11.5	Application and Presentation Layer	16
1.12	A Block and Its Structure	17
1.12.1	A Block	17
1.12.2	Block Structure	17
1.12.3	Ledger	18
1.12.4	Distributed	19
1.12.5	Transparency	19
1.12.6	Confirmation	20
1.12.7	Proof of Work	20
1.12.8	Block Awards	20
1.12.9	Transactions and UTXOs	21
1.12.10	Consensus	22

1.13	Scaling Blockchain	23
1.13.1	Issues in Scaling	23
1.13.2	Off-Chain Computation	24
1.13.3	Sharding in Blockchain	24
1.14	Blockchain DApps and Usecases	25
1.15	Laboratory Work	25
1.15.1	Program for Implementing Blockchain in Python	26
1.15.2	Program for Mining a New Block in Blockchain and Printing It	28
1.15.3	Program for Creating Four Blocks in Blockchain and Printing and Traversing	30
1.15.4	Implementing Blockchain and Printing All Fields as per Etherscan.io	32
1.15.5	Implementing Blockchain and UTXo in Python	35
1.15.6	Explanation of Code	37
1.15.7	Implementation of PoW Algorithm in Python	37
1.15.8	Implementation of PoS Algorithm in Python	40
1.15.9	Program to Fetch the Latest Block Information from Ethereum Blockchain Using Etherscan API	42
1.15.10	Explanation of Code	43
1.16	Summary	44
1.17	Exercise	44
1.17.1	Multiple Choice Questions	44
1.17.2	Short Answer Questions	45
1.17.3	Long Answer Questions	46
1.17.4	Practical Questions	46
1.17.5	Answer Set of MCQ	46
2	Essentials of Blockchain Programming	47
2.1	Cryptography Primitives	47
2.1.1	Hash Function	47
2.2	Hash Functions	47
2.2.1	Properties of Hash Functions	48
2.2.2	Hash Pointers and Data Structures	48
2.2.3	Tampering Is Computationally Challenging	49
2.2.4	Role of Hashes in Blockchain	51
2.3	Secure Hash Algorithm (SHA)	53
2.3.1	SHA Algorithm	53
2.3.2	Hashing Patterns	54
2.4	Public Key Cryptography	54
2.4.1	Secure Hash Algorithm-3 (Keccak)	55
2.5	Merkle Tree	56
2.5.1	Merkle Tree Creation	57
2.5.2	Role of Merkle Tree in Blockchain	57
2.5.3	Structure of Merkle Tree	58
2.5.4	Merkle Proof	58
2.5.5	Proof of Membership	59
2.5.6	Proof of Nonmembership	59

2.5.7	Advantages of Merkle Trees	60
2.5.8	Applications of Merkle Trees	60
2.5.9	Merkle Tree Proof of Reserves	60
2.6	Public Key Cryptography	61
2.6.1	Public and Private Keys	61
2.6.2	Public Key Encryption Algorithms	61
2.6.3	Digitally Signed Transaction	62
2.6.4	Digital Signing in Blockchain	62
2.7	Laboratory Work	63
2.7.1	Program in Python that Demonstrates the Use of Hashlib Library to Generate the SHA-3 Hash of a Message	63
2.7.2	Python Program that Takes a String and the Desired Number of Leading Zeros from the User and Outputs the Input String, the Nonce Value for Which the Leading Zeros Puzzle Is Solved, and the Corresponding Hash Generated	64
2.7.3	Program to Create Hash Code from Given Input String	65
2.7.4	Program in Python that Demonstrates How to Use the SHA-256 Hash Function and Its Application in a Simple Blockchain	66
2.7.5	Write a Program in Python to Verify Hash Properties	67
2.7.6	Program to Demonstrate a Simple Implementation of a Blockchain Using Hash Codes as a Chain of Blocks	68
2.7.7	Program to Demonstrate the Mining Process in Blockchain	70
2.7.8	Program to Create a Merkle Tree in Blockchain	72
2.7.9	Program to Prove Membership and Nonmembership in a Merkle Tree Blockchain	73
2.7.10	Explanation of Code	75
2.7.11	Program to Demonstrate How to Prove the Membership and Nonmembership of an Element in a Merkle Tree Blockchain	75
2.7.12	Program in Python that Demonstrates RSA Digital Signature Scheme	76
2.8	Summary	78
2.9	Exercise	78
2.9.1	Multiple Choice Questions	78
2.9.2	Short Answer Questions	80
2.9.3	Long Answer Questions	80
2.9.4	Practical Questions	80
2.9.5	Programming Questions	80
3	Bitcoin	83
3.1	What Is Bitcoin	83
3.2	History	83
3.3	Predicted Market	84
3.4	Wallet	84
3.4.1	Bitcoin Wallets	85
3.4.2	Custodial Wallet	85
3.4.3	Noncustodial Wallet	86
3.4.4	Software Wallet	86
3.4.5	Hardware Wallet	86
3.4.6	Features of Digital Wallet	87

3.4.7	Difference Between Digital Wallet and Bank Accounts	87
3.4.8	Top Digital Wallet	87
3.5	Digital Keys and Addresses	88
3.5.1	Private Keys	89
3.5.2	Public Keys	89
3.6	Addresses in Bitcoin	90
3.7	Transaction	91
3.7.1	Transaction Lifecycle	91
3.7.2	Creating Transactions	91
3.7.3	Broadcasting Transactions to the Bitcoin Network	91
3.7.4	Propagating Transactions on the Bitcoin Network	92
3.7.5	Data Structures for Transaction	92
3.7.6	Types of Transactions	93
3.7.7	Transaction Input and Output	94
3.8	Digital Signature	94
3.9	Mining and Consensus in Bitcoin	95
3.9.1	Mining	95
3.9.2	Consensus	95
3.9.3	Decentralized Consensus in Bitcoin	96
3.9.4	Mining and Racing in Bitcoin	97
3.9.5	Cost of Mining in Bitcoin	98
3.9.6	Consensus Attacks in Bitcoin	99
3.10	Forking	101
3.10.1	Hard Fork	101
3.10.2	Soft Fork	101
3.11	Laboratory Work	102
3.11.1	Program to Generate Private Keys Securely on a Hardware Wallet	102
3.11.2	Program to Generate Public-Private Key Pairs, Encrypting and Storing Private Keys Securely and Signing Transactions Using the Private Key	103
3.11.3	Program to Demonstrate Some of the Features of a Digital Wallet	104
3.11.4	Program to Compare the Features of Popular Digital Wallets, Rank Them Based on User Reviews and Ratings, and Recommend a Digital Wallet Based on User Preferences	105
3.11.5	Program to Deploy a Smart Contract to Blockchain Using a Tool Like Remix IDE	107
3.11.6	Program that Measures the Transaction Throughput of EOA–EOA Transactions and CA–CA Transactions Using Various Gas Limits on the Ethereum Network	108
3.11.7	Program that Uses Web3 to Categorize Ethereum Addresses as EOA or Contract Addresses and Evaluates Its Accuracy and Performance on a Large Dataset of Addresses	110
3.11.8	Program that Simulates the Life Cycle of a Transaction on the Ethereum Network and Measures the Time and Resources Required	111
3.11.9	Program for Implementing ECDSA	112
3.11.10	Program to Create a Bitcoin Transaction and Sign It with a SIGHASH Flag Using the bitcoinlib Library	112
3.11.11	Program for Bitcoin Mining	113

3.11.12	Program that Demonstrates How to Identify 51% Attacks on a Blockchain	115
3.11.13	Program to Demonstrate the Concept of Forking	116
3.11.14	Program to Detect and Deal with 51% Attacks in the Bitcoin Blockchain	118
3.12	Summary	119
3.13	Exercise	119
3.13.1	Multiple Choice Questions	119
3.13.2	Short Answer Questions	120
3.13.3	Long Answer Questions	121
4	Ethereum Blockchain	123
4.1	Overview of Ethereum Blockchain	123
4.1.1	Key Features	124
4.1.2	EVM	125
4.2	History of Ethereum	125
4.2.1	Ledger to State Machine	125
4.2.2	Ethereum Network	127
4.3	Smart Contracts	128
4.4	Challenges in Implementing Smart Contracts	129
4.4.1	Smart Contract Life Cycle	129
4.4.2	Introducing Solidity	130
4.4.3	Global Variables	131
4.5	Ethereum Development Tools	134
4.6	Ethereum Transactions	135
4.6.1	Transaction Life Cycle	136
4.7	Gas and Transaction Fees	136
4.7.1	Addressing Gas Fees	136
4.7.2	Factors Affecting Gas Price	137
4.7.3	Calculating Gas Costs	137
4.7.4	Gas Fee Calculation	138
4.7.5	Implications of Base Fee	138
4.7.6	Transaction Cost Predictability	138
4.7.7	Future with PoS	138
4.7.8	Gas Fees and Orchid	139
4.7.9	Example 1: Wallet-to-Wallet Transfer	139
4.7.10	Example 2: Deploying a Simple Contract	139
4.7.11	Avoiding Ethereum Gas Fees	140
4.8	Laboratory Work	141
4.8.1	Solidity Program for Displaying Hello Message	141
4.8.2	Program for Demonstrating Simple Increment and Decrement Functions	142
4.8.3	Smart Contract Development with Solidity	143
4.8.4	Implementing Security Measures in Smart Contracts	145
4.8.5	Developing an ERC-20 Token	147
4.8.6	Building a Simple DApp	150
4.8.7	Interacting with Off-Chain Data Using Oracles	151

- 4.8.8 Program to Demonstrate a Basic Example of Smart Contract Interaction and Ownership Management on Ethereum Blockchain 153
- 4.8.9 Program to Create a Decentralized Blind Auction Smart Contract on the Ethereum Blockchain, Enabling Participants to Place Concealed Bids, Reveal Them, and Determine the Highest Bidder While Ensuring Secure Fund Management and Transparent Auction Outcomes. This Contract Facilitates a Trustless and Tamper-Resistant Auction Mechanism, Promoting Fairness and Efficiency in Auction Processes 155
- 4.8.10 Program to Showcase the Vulnerability of Reentrancy Attacks in a Smart Contract Context and Demonstrate the Implementation of a Solution Using a Reentrancy Guard 160
- 4.9 Mist Browser 162
 - 4.9.1 Guidelines for Using Mist Browser 162
 - 4.9.2 Mist and Geth 163
 - 4.9.3 Geth’s Role 163
- 4.10 Summary 163
- 4.11 Exercise 164
 - 4.11.1 Multiple Choice Questions 164
 - 4.11.2 Long Answer Questions 165
- 5 Hyperledger** 167
 - 5.1 Introduction to Hyperledger 167
 - 5.1.1 The Purpose of Hyperledger 167
 - 5.2 Hyperledger Architecture 168
 - 5.2.1 Infrastructure Layer 168
 - 5.2.2 Framework Layer 169
 - 5.2.3 Tool Layer 170
 - 5.3 Hyperledger Community and Development 170
 - 5.4 Hyperledger Smart Contracts (Chaincode) 170
 - 5.5 The Functioning of Hyperledger 171
 - 5.5.1 Contributor 171
 - 5.5.2 Endorser 171
 - 5.5.3 Consenter 171
 - 5.5.4 Example 171
 - 5.5.5 Advantages of Hyperledger 171
 - 5.5.6 Limitations of Hyperledger 173
 - 5.6 Hyperledger Projects 173
 - 5.6.1 Comparison of Hyperledger with Other Blockchain Frameworks 174
 - 5.6.2 Hyperledger Fabric in Blockchain 177
 - 5.6.3 Consensus in Hyperledger Fabric 178
 - 5.7 Hyperledger Consortiums and Networks 180
 - 5.8 Hyperledger and Blockchain as a Service (BaaS) 181
 - 5.8.1 Hyperledger Adoption Through BaaS 181
 - 5.8.2 Advantages and Considerations 182
 - 5.9 Laboratory Work 182
 - 5.9.1 Program to Demonstrate Interaction with a Hyperledger Fabric Blockchain Network Using the Hyperledger Fabric JavaScript SDK 182

5.9.2	Program to Demonstrate How Hyperledger Fabric Could Be Used in a Healthcare Context to Manage Patient Medical Records	184
5.9.3	Program to Demonstrate the Implementation of a Basic Government Application Using Hyperledger Fabric	187
5.9.4	Program to Demonstrate Finance Application Using Hyperledger Fabric	188
5.9.5	Program to Demonstrate the Implementation of a Finance and Payments System Using Hyperledger Fabric	190
5.9.6	Explanation of Code	193
5.9.7	Program to Demonstrate Simple Interoperability Using the Hyperledger Fabric JavaScript SDK to Interact with the Network and Demonstrate How Two Different Smart Contracts Can Work Together	194
5.9.8	Program to Demonstrate Smart Contract Modeling with Composer and Docker	195
5.9.9	Program for Demonstrating Hyperledger Caliper, a Benchmarking Tool That Measures the Performance of Hyperledger Blockchain Applications Under Various Conditions	197
5.9.10	Running Caliper Benchmarks with Docker	197
5.10	Summary	198
5.11	Exercise	198
5.11.1	Multiple Choice Questions	199
5.11.2	Short Answer Questions	200
5.11.3	Long Answer Questions	200
5.11.4	Programming Questions	201
6	Case Studies Using Blockchain	203
6.1	Blockchain – The Technology for Document Management	203
6.1.1	The Ownership	203
6.1.2	Introduction and Background	203
6.1.3	Problem Statement	204
6.1.4	Use Case Description	204
6.1.5	Solution Architecture	204
6.1.6	Implementation Steps	205
6.1.7	Smart Contracts	206
6.1.8	Data Management and Security	206
6.1.9	Interoperability and Integration	206
6.1.10	User Experience	206
6.1.11	Results and Benefits	207
6.1.12	Challenges and Lessons Learned	207
6.1.13	Future Enhancements and Scalability	207
6.1.14	Conclusion	207
6.2	Case Study 2: Blockchain in the Food Supply Chain	208
6.2.1	Introduction and Background	208
6.2.2	Problem Statement	208
6.2.3	Use Case Description	208
6.2.4	Solution Architecture	208
6.2.5	Implementation Steps	209
6.2.6	Smart Contracts	210

6.2.7	Data Management and Security	210
6.2.8	Interoperability and Integration	210
6.2.9	User experience	210
6.2.10	Results and Benefits	210
6.2.11	Challenges and Lessons Learned	211
6.2.12	Future Enhancements and Scalability	211
6.2.13	Conclusion	211
6.3	Case Study 3: Blokchain in the Insurance Industry	211
6.3.1	Introduction and Background	211
6.3.2	Problem Statement	212
6.3.3	Use Case Description	212
6.3.4	Solution Architecture	212
6.3.5	Implementation Steps	212
6.3.6	Smart Contracts	212
6.3.7	Data Management and Security	214
6.3.8	Interoperability and Integration	214
6.3.9	User Experience	215
6.3.10	Analysis	215
6.3.11	Conclusion	215
6.4	Case Study 4: India's Income Tax Department's Simplification of Tax Procedures	215
6.4.1	Introduction and Background	215
6.4.2	Problem Statement	216
6.4.3	Use Case Description	216
6.4.4	Solution Architecture	216
6.4.5	Implementation Steps	216
6.4.6	Smart Contracts	217
6.4.7	Tax Authority Interaction (Not Implemented in This Simplified Example)	218
6.4.8	Event Log	218
6.4.9	Data Management and Security	218
6.4.10	Interoperability and Integration	218
6.4.11	User Experience	219
6.4.12	Analysis	219
6.4.13	Conclusion	219
6.5	Case Study 5: Retail Banking	220
6.5.1	Introduction and Background	220
6.5.2	Problem Statement	220
6.5.3	Use Case Description	221
6.5.4	Solution Architecture	221
6.5.5	Implementation	221
6.5.6	Data Management and Security	222
6.5.7	Network Security	223
6.5.8	Incident Response	223
6.5.9	Interoperability and Integration	223
6.5.10	User Experience	224
6.5.11	Analysis	224
6.5.12	Conclusion	225
6.6	Summary	225

6.7	Exercise	226
6.7.1	Multiple Choice Questions	226
6.7.2	Short/Long Answer Questions	227
7	Beyond Blockchain	229
7.1	Blockchain for the Metaverse	229
7.2	Emergence of the Metaverse	229
7.3	Understanding the Metaverse	230
7.4	Metaverse Layers	230
7.4.1	Spatial Computing	231
7.4.2	Metaverse Components	232
7.5	Metaverse Through Immersive Technologies	233
7.5.1	Challenges in Metaverse Implementation	234
7.6	Blockchain’s Role in the Metaverse	236
7.6.1	Why Blockchain Technology Is Crucial for the Metaverse	236
7.6.2	Interoperability and Standards	237
7.6.3	Security and Trust	237
7.6.4	Monetization and Incentives	237
7.7	Digital Scarcity and Ownership of Virtual Assets	237
7.8	Building Trust and Security in the Decentralized Metaverse	238
7.8.1	Trustless Nature of the Metaverse	238
7.8.2	Zero Trust Security in the Metaverse	238
7.9	Data Hub for Crypto, DeFi, NFT, Metaverse	239
7.9.1	Real-Time Data Streaming	239
7.10	Digital Trust Networks	240
7.10.1	Diverse Applications of Digital Trust Networks	240
7.10.2	Peer-to-Peer Marketplaces	241
7.10.3	Platform Ecosystems	241
7.10.4	Zero Trust Security Systems	241
7.10.5	Digital Identity Platforms	241
7.10.6	Decentralized Autonomous Organizations	241
7.11	Beyond Cryptocurrency: Transforming ESG, Digital Assets, and Financial Markets	241
7.11.1	Environmental, Social, and Governance (ESG)	242
7.11.2	Digital Assets and Currency	242
7.11.3	Central Bank Digital Currencies	242
7.11.4	Blockchain Modernizing Financial Markets	242
7.11.5	Blockchain and AI: A Synergy for Trust and Intelligence	243
7.11.6	Data Analysis and Predictive Insights	243
7.11.7	Smart Contract Automation	243
7.11.8	Enhanced Security	243
7.11.9	Scalability and Performance	243
7.12	The Future of Banks	244
7.12.1	Instant and Efficient Cross-Border Payments	244
7.12.2	Streamlined Trade Finance	244
7.12.3	Innovative Revenue Streams	244

7.13	Blockchain and Sustainable Technologies	244
7.13.1	Renewable Energy Trading	245
7.13.2	Environmental Conservation	245
7.14	Tangle	246
7.15	Summary	247
7.16	Short/Long Answer Questions	248
Bibliography	249
Index	253

About the Authors



Dr. Ramchandra Mangrulkar is a Professor in the Department of Information Technology in the Dwarkadas J. Sanghvi College of Engineering in Mumbai, India. He holds various memberships in professional organizations such as IEEE, ISTE, ACM, and IACSIT. He completed his Doctor of Philosophy (Ph.D.) in Computer Science and Engineering from S.G.B. Amravati University in Maharashtra and Master of Technology (MTech) in Computer Science and Engineering from the National Institute of Technology, Rourkela. Dr. Mangrulkar is proficient in several technologies and tools, including Microsoft’s Power BI, Power Automate, Power Query, and Power Virtual Agents, Google’s Dialog Flow, and Overleaf. With over 22 years of combined teaching and administrative experience, Dr. Mangrulkar has established himself as a knowledgeable and skilled professional in his field. He has also obtained certifications like Certified Network Security Specialist International CyberSecurity Institute (ICSI) – Certified Network Security Specialist (CNSS) from ICSI, UK. Dr. Mangrulkar has an extensive publication record, with 95 publications including refereed/peer-reviewed international journal publications, book chapters with international publishers (including ones indexed in Scopus), and international conference publications.



Dr. Pallavi Vijay Chavan is Associate Professor at Ramrao Adik Institute of Technology, D. Y. Patil “Deemed-to-be-University,” Navi Mumbai, MH, India. She has been in academia for the past 17 years working in the area of computing theory, data science, and network security. In her academic journey, she has published research in data science and security with reputable publishers such as Springer, Elsevier, CRC Press, and Inderscience. She has published 2 books, over 7 book chapters, more than 10 international journal papers, and over 30 international conference papers. Presently she serves as advisor to five Ph.D. research scholars in related fields. She completed her Ph.D. at Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, MH, India, in 2017. In 2003,

she earned the first merit position at Nagpur University for a B.E. in Computer Engineering. She is the recipient of research grants from University Grants Commission (UGC), Council of Scientific & Industrial Research (CSIR), and University of Mumbai. She serves as a reviewer for Elsevier and Inderscience journals. Her motto is “Teaching is a mission.”

About the Technical Reviewer



Dr. Parikshit Mahalle is a senior member of the Institute of Electrical and Electronics Engineers and Professor, Dean of Research and Development and -Chair of the Department of Artificial Intelligence and Data Science at Vishwakarma Institute of Information Technology, Pune, India. He completed his Ph.D. at Aalborg University, Denmark, and continued as a postdoctoral researcher at Communication, Media & Information Technologies, Copenhagen, Denmark. He has over 23 years of teaching and research experience. He is a former member of the Board of Studies in Computer Engineering and former chairman of the Department of Information Technology at Savitribai Phule Pune University and various universities and autonomous colleges throughout India. He owns 15 patents, has published over 200 research studies and papers (2950+ Google Scholar, 1550+ H index-25 and Scopus citations, 438 H index-8, Web of Science, and H index-10 citations), and has authored/edited 56 books with Springer, CRC Press, Cambridge University Press, and others. He is editor in chief for IGI Global's *International Journal of Rough Sets and Data Analysis* and Inderscience's *International Journal of Grid and Utility Computing*, is a member of the editorial review board for IGI Global's *International Journal of Ambient Computing and Intelligence*, and serves as a reviewer for various reputable journals and conferences. His research interests include machine learning, data science, algorithms, Internet of Things, identity management, and security. He currently advises eight Ph.D. students in the areas of IoT and machine learning, and six students have successfully defended their Ph.D. under his supervision from Savitribai Phule Pune University. He is also the recipient of the Best Faculty Award by Sinhgad Institutes and Cognizant Technology Solutions. He has delivered over 200 lectures at the national and international levels.

Preface

Blockchain has become the buzzword of the day. Developers are focusing on more user-friendly applications with the help of blockchain, achieving decentralization and a trustless environment without third-party involvement. This includes diverse concepts and tools that play major roles in developing crypto-based applications in various programming languages. The distributed ledger and smart contracts involved reveal the importance of blockchain in creating immutable and transparent, cryptographically secure record-keeping of transactions. The programming approach helps to shed light on the core concepts of blockchain and relevant applications in easy steps. This helps to motivate learners to become part of the solution to most of the applications demanding trustless and independent autonomous systems. The identification and examination of blockchain technology beyond cryptocurrency will help to investigate alternative solutions using many blockchain-supportive tools.

The main purpose of this book is to present the difficult concepts of blockchain technology in very accessible and easy-to-understand language using a programming approach so that learners can easily grasp the key concepts arising from the emerging notion of blockchain technology. Another purpose of this book is to make available the experience of academia and industry to the target audience through hands-on programming.

This book presents the concepts of blockchain technology in a concise manner with clear and easy examples using trending blockchain programming languages. The book fills a gap of address issues surrounding the practical implementation of blockchain concepts using case studies. The book also highlights the usefulness of blockchain technology beyond its current applications.

Mumbai, India
September 2023

Ramchandra Sharad Mangrulkar
Pallavi Vijay Chavan

Acknowledgements

We extend our sincere gratitude to the dedicated contributors and accomplished researchers in the field of blockchain for their invaluable contributions and pioneering work.



Readers of this book are likely to have some knowledge and basic idea about the enormous potential of the trending, decentralizing, and trustworthy technology called blockchain. This technology represents an innovation in the digital ecosystem that has significantly impacted trusted computing activities, resulting in an enhanced level of protection from cyber security threats.

This chapter lays out the fundamentals of blockchain technology, presenting its theoretical background, historical milestones, and present growth trends. Further, the conceptual view of a block in blockchain and the types of blockchain are described. The chapter discusses the basic skill set and libraries required to start doing “blockchain programming,” which is a key objective of this book. The chapter ends with a few examples and their implementation in Python.

1.1 Prerequisites

The prerequisites for blockchain technology include:

- **Understanding of cryptography:** Cryptography is the foundation of blockchain technology. A basic understanding of cryptographic concepts, such as hashing, public-key encryption, and digital signatures, is necessary.
- **Distributed systems:** Blockchain is a distributed system that runs on multiple nodes. Therefore, it is essential to have a good understanding of distributed systems to build and deploy blockchain applications.
- **Data structures and algorithms:** Blockchain technology relies on complex data structures such as Merkle trees and algorithms such as consensus algorithms. Understanding of these concepts is crucial for building a robust blockchain system.
- **Networking and security:** Blockchain technology requires a good understanding of networking protocols, such as TCP/IP, HTTP, and HTTPS. Additionally, a solid understanding of security concepts, such as firewalls, encryption, and authentication, is necessary to develop secure blockchain applications.
- **Smart contracts:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller directly written into lines of code. Knowledge of smart contract programming languages, such as Solidity, is necessary for building decentralized applications.

- **Business and economics:** Blockchain technology is disrupting traditional business models and creating new opportunities. Understanding the economics of blockchain and how it can be applied to business is essential for leveraging its potential.
- **Legal and regulatory dimensions:** Blockchain technology operates in a regulatory gray area in many countries, and regulations are constantly evolving. Understanding the legal and regulatory environment in which blockchain operates is critical for creating compliant and successful blockchain applications.

1.2 Blockchain Myths

Blockchain is an emerging technology. The following list dispels some of the myths surrounding blockchain:

- **Blockchain is the same thing as Bitcoin (or any other cryptocurrency)**
There is a misleading idea that if you learn blockchain technology, you will become a good trader! This is untrue. Blockchain is not equivalent to any cryptocurrency, whether Bitcoin or any other currencies on the market like Altcoins. In fact, blockchain is a technology, whereas Bitcoin is a cryptocurrency that makes use of blockchain technology. Blockchain has many applications outside the crypto world. Blockchain technology provides a full support system for developing cryptocurrencies, whereas Bitcoin is a fundamental application that builds on this emerging blockchain technology.
- **Blockchain can solve all security issues**
Blockchain cannot be used to definitively eliminate corruption or fraudulent activities. Blockchain's many applications have been developed by players in the various models governing economies around the world. Blockchain cannot all issues related to security. Solving all societal issues using blockchain is a formidable challenge. Thus, careful consideration needs to be given as to which societal issues should be addressed using blockchain.
- **Blockchain is the only possible technology**
Blockchain is not necessarily the best technology for solving your problems; they might be better solved employing technology that does not use blockchain. It is possible that many different existing technologies would yield better results in terms of security without the use of blockchain.
- **Blockchain and distributed databases are similar technologies**
Blockchain and distributed databases are different technologies. Blockchain is not a distributed databases. Blockchain is not designed to store and secure data. Blockchain and distributed databases are two different technologies, each with its own merits and demerits and different potential to solve different problems. Both are essential, and one cannot easily replace the other.

1.3 Blockchain and Decentralization

Blockchain technology emerged to solve most of the issues in decentralization. Decentralization refers to the distribution of power or authority away from a single central entity to multiple individuals or groups. In the context of technology, it refers to systems or networks that operate without a central authority controlling them. Figure 1-1 gives an overview of centralized and decentralized systems.

Decentralization is required to address trust issues, that is, the different parties involved do not trust each other, but they should cooperate. The network of different entities such as businesses, individuals, government, private- and public-sector organizations, with their own interests, can come

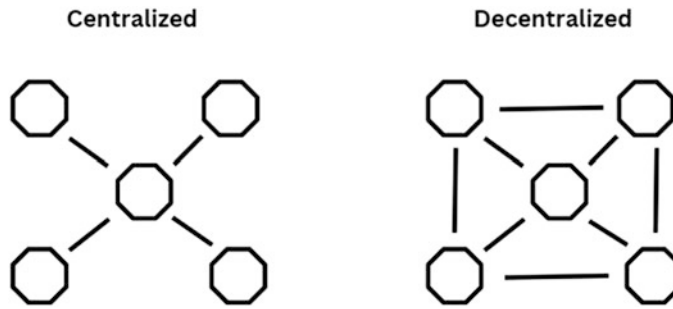


Figure 1-1 Overview: centralized and decentralized systems

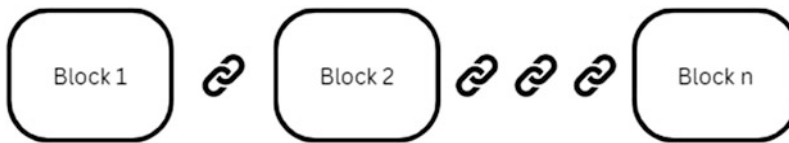


Figure 1-2 Blocks and chain in blockchain

together and cooperate with each other to solve societal issues. Decentralization and blockchain work together to create a secure, transparent, and tamper-proof system that operates without the need for a central authority.

1.4 What Is Blockchain?

Blockchain is an append-only, immutable, never-ending chain of data where data, once added, cannot be deleted or modified, achieving a tamper-proof system. The immutable property of blockchain means no one can change it. Its append-only nature ensures that no one can erase data once they are written in the blockchain. This append-only nature of blockchain makes it a never-ending but fully traceable system. Figure 1-2 shows the basic idea of blocks and chain in blockchain.

Every individual player maintains a copy of the blockchain, removing the need for central administration or centralization. The addition of information to the existing blockchain happens in the form of a new block appended at the end while at the same time ensuring that all copies of the local blockchain available to the different network players must also be updated in the same order. This will ensure data consistency in the blockchain, and all copies will be the same. This doubtlessly will require an additional authentication and validation mechanism, but at a superficial level, everyone will have an updated copy of the blockchain.

The data structure in blockchain consists of a chain of blocks linked together with the help of current and previous pointers. These two fields store the hashed data of the contents of the block, the previous pointer stores the hashed data of the previous block, and the current pointer stores the hashed data of the current block.

The data are stored in the blockchain in a transparent way and are available to everyone, allowing anyone to validate and verify the data as and when required.

Definition 1.1 Blockchain is a decentralized, immutable, append-only public ledger.

1.5 Disruptive Technology

Clayton Christensen introduced the idea of disruptive technologies in a 1995 *Harvard Business Review* article. Disruptive technology refers to any innovation that disrupts an existing market or industry, displacing established products or services and creating new markets and opportunities. These technologies often have a transformative effect on society, leading to changes in business models, consumer behavior, and even cultural norms.

Not all innovations are disruptive technologies. It is the process rather than product or services. Blockchain is a sustaining innovation rather than a disruptive innovation in the financial sector.

Disruptive technologies typically emerge from unexpected sources and are often initially dismissed as inferior or irrelevant by established players in the market. However, as they gain momentum and become more widely adopted, they can completely change the competitive landscape and reshape entire industries.

The following are examples of disruptive technologies:

- **Ecommerce:** The rise of ecommerce in the 2000s disrupted traditional brick-and-mortar retail, creating new opportunities for businesses to sell products and services online.
- **Personal computers:** The development of personal computers in the 1970s and 1980s disrupted the established mainframe computer industry, creating new markets and opportunities for businesses and individuals.
- **Social media:** The emergence of social media in the 2010s disrupted traditional media and advertising industries, leading to the rise of new platforms for content creation and distribution.
- **Digital photography:** The advent of digital photography in the 1990s disrupted the traditional film photography industry, leading to the demise of many established companies and the emergence of new players in the market.

Blockchain is considered a disruptive technology for several reasons:

- **Decentralization:** One of the key features of blockchain technology is its ability to operate in a decentralized manner, without the need for intermediaries such as banks or government institutions. This eliminates the need for trust in centralized institutions, which can be slow, expensive, and prone to corruption.
- **Immutable and transparent:** Blockchain technology is immutable and transparent, meaning that once data are added to a blockchain, it cannot be modified or deleted. This creates a high degree of trust in the data stored on the blockchain and eliminates the need for intermediaries to verify data.
- **Security:** Blockchain technology is secured by cryptographic algorithms that make it virtually impossible to tamper with the data stored on the blockchain. This creates a high degree of security for transactions and other data stored on the blockchain.
- **Smart contracts:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This eliminates the need for intermediaries to execute and enforce contracts, which can be slow, expensive, and prone to errors.
- **Tokenization:** Blockchain technology enables the creation and exchange of digital assets, or tokens, which can represent anything of value, such as currency, property, or ownership rights. This creates new opportunities for businesses to generate value and disrupt traditional business models.

1.6 History

Blockchain, a technology with the potential to become the foundation of global record-keeping systems, was introduced a mere decade ago by anonymous individuals associated with the digital currency Bitcoin, under the pseudonym Satoshi Nakamoto. Despite its relatively recent inception, blockchain has quickly gained recognition as a transformative innovation, poised to revolutionize various industries through its decentralized and secure nature.

1.6.1 Milestones in Blockchain Development

The subsection discusses some of the significant milestones in the development of blockchain technology (Figure 1-3).

1. 2008 – The publication of Bitcoin’s whitepaper by Satoshi Nakamoto marked the groundbreaking introduction of the cryptocurrency. This event revolutionized the financial landscape, ushering in a new era of decentralized digital currency. The whitepaper laid the foundation for a peer-to-peer electronic cash system that would eventually disrupt traditional monetary systems worldwide.
2. 2009 – The inaugural Bitcoin transaction between Satoshi Nakamoto and Hal Finney stands as a significant milestone in cryptocurrency history. This historic event symbolized the practical application and transferability of Bitcoin as a digital currency. The transaction showcased the

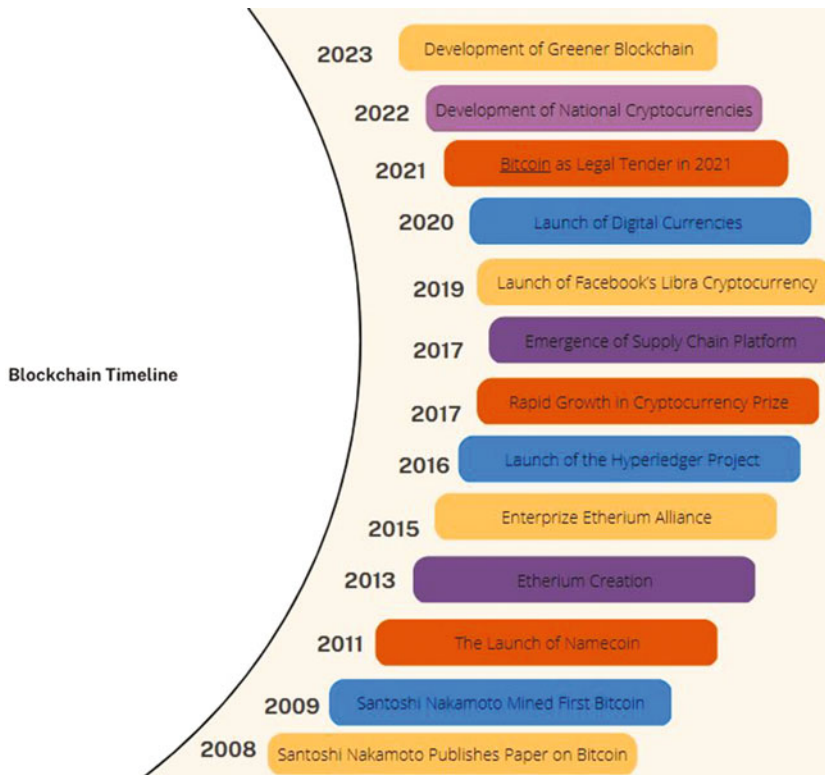


Figure 1-3 Blockchain timeline

potential of Bitcoin as a decentralized payment system, setting the stage for its widespread adoption and subsequent impact on the financial industry.

3. 2011 – Namecoin’s launch marked a groundbreaking moment as it became the first alternative cryptocurrency to utilize blockchain technology. This pioneering step opened the door for a multitude of innovative blockchain-based digital assets. Namecoin’s introduction demonstrated the potential for decentralized systems beyond traditional currencies, paving the way for the development of various blockchain applications and cryptocurrencies.
4. 2013 – Vitalik Buterin’s creation of Ethereum unleashed a revolutionary platform enabling the creation of smart contracts and decentralized applications (dApps). Ethereum’s emergence introduced a new paradigm in blockchain technology, empowering developers to build complex applications on a decentralized network. Buterin’s vision laid the foundation for a vibrant ecosystem of dApps, fueling innovation and transforming industries through the power of decentralized computing.
5. 2015 – The formation of the Enterprise Ethereum Alliance united leading corporations and blockchain startups, fostering collaboration in the advancement of blockchain technology. This alliance served as a catalyst for exploring the potential of Ethereum in various industries and promoting blockchain adoption on a global scale. The Enterprise Ethereum Alliance aimed to accelerate innovation, establish industry standards, and drive the mainstream integration of blockchain solutions across sectors.
6. 2016 – The Hyperledger Project, initiated by the Linux Foundation, set out to develop open-source blockchain software specifically tailored to enterprise applications. This strategic launch brought together industry leaders and technologists to collaborate on building scalable and interoperable blockchain solutions. By providing a collaborative platform, the Hyperledger Project aimed to accelerate the adoption of blockchain technology among businesses, fostering transparency, efficiency, and trust in enterprise operations.
7. 2017 – The cryptocurrency market witnessed an unprecedented surge in value, primarily led by Bitcoin, accompanied by an explosive growth in initial coin offerings (ICOs). This phenomenon resulted in widespread frenzy and speculation, attracting investors seeking to capitalize on the potential returns of digital assets. The soaring value of cryptocurrencies and the ICO boom reshaped the financial landscape, bringing both opportunities and risks while fueling the development of innovative blockchain projects worldwide.
8. 2018 – Blockchain-based platforms like IBM’s Food Trust have emerged as transformative solutions for supply chain management, enabling enhanced transparency and traceability within the food industry. By leveraging blockchain technology, these platforms offer a secure and immutable record of every step in the supply chain, promoting accountability and reducing fraud. The adoption of such blockchain solutions has the potential to revolutionize the way we track and verify the origins, quality, and safety of food products, ensuring consumer confidence and driving industry-wide improvements.
9. 2019 – Facebook’s launch of the Libra cryptocurrency encountered substantial regulatory scrutiny and widespread resistance from governments worldwide. The ambitious project aimed to create a global digital currency, but concerns over data privacy, monetary sovereignty, and potential risks to the financial system led to intense pushback. The Libra initiative highlighted the complex challenges and regulatory hurdles that arise when tech giants venture into the realm of cryptocurrencies and sparked discussions on the future of digital currencies in a regulated environment.
10. 2020 – Major financial institutions like JP Morgan and Goldman Sachs have embraced blockchain technology, recognizing its potential for efficiency and security in financial operations. Simultaneously, numerous countries have launched their own central bank digital currencies (CBDCs),

aiming to leverage the benefits of blockchain and enhance their monetary systems. This combined trend showcases the growing acceptance and integration of blockchain technology within the traditional financial sector, paving the way to transformative changes in how transactions and currencies are managed globally.

11. 2021 – In a historic move, El Salvador became the first country to officially adopt Bitcoin as legal tender in 2021. This decision enabled businesses to utilize Bitcoin for paying employee salaries and established its acceptance as a valid payment method throughout the country. El Salvador’s embrace of Bitcoin as a form of currency marked a significant milestone in the mainstream acceptance and integration of cryptocurrencies into national economies.
12. 2022 – The year 2022 witnessed notable blockchain growth, particularly in the emergence of national cryptocurrencies. This concept revolved around the idea of CBDCs, where central banks opted to develop their own digital coins instead of relying on decentralized cryptocurrencies. This trend highlighted a shift toward more centralized control over digital currencies, with central banks exploring the benefits and challenges of issuing their own blockchain-based currencies.
13. 2023 – The year 2023 has witnessed a notable focus on environmentally friendly blockchains, facilitated by carbon offsetting practices and energy-conscious network architectures. The adoption of greener blockchains will be made more feasible through the utilization of eco-friendly algorithms like proof of stake. These developments signify a growing commitment to reducing the environmental impact of blockchain technology and promoting sustainable practices within the industry.

1.7 Features of Blockchain

The remarkable attention and interest surrounding blockchain technology can be attributed to several key factors (Figure 1-4).

1. Immutable

Immutability lies at the core of blockchain technology, rendering it an unchangeable and enduring network. By operating through a network of nodes, the blockchain ensures that once a transaction is recorded, it becomes permanent and resistant to modification. This immutability characteristic establishes the blockchain as a secure and trustworthy ledger, bolstering confidence in its integrity and authenticity.

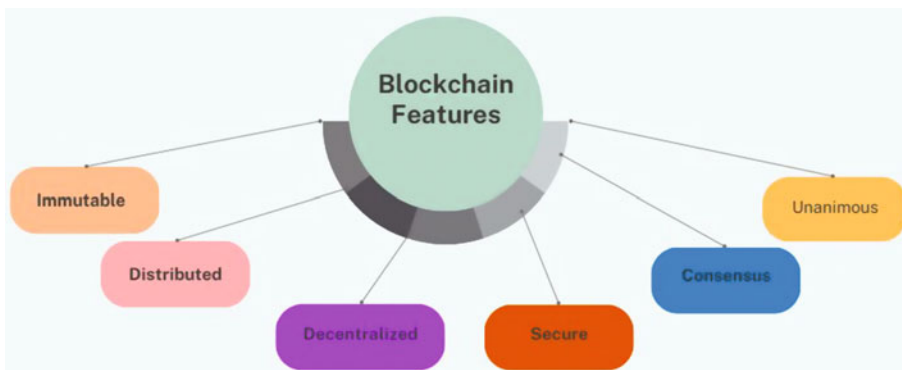


Figure 1-4 Features of blockchain