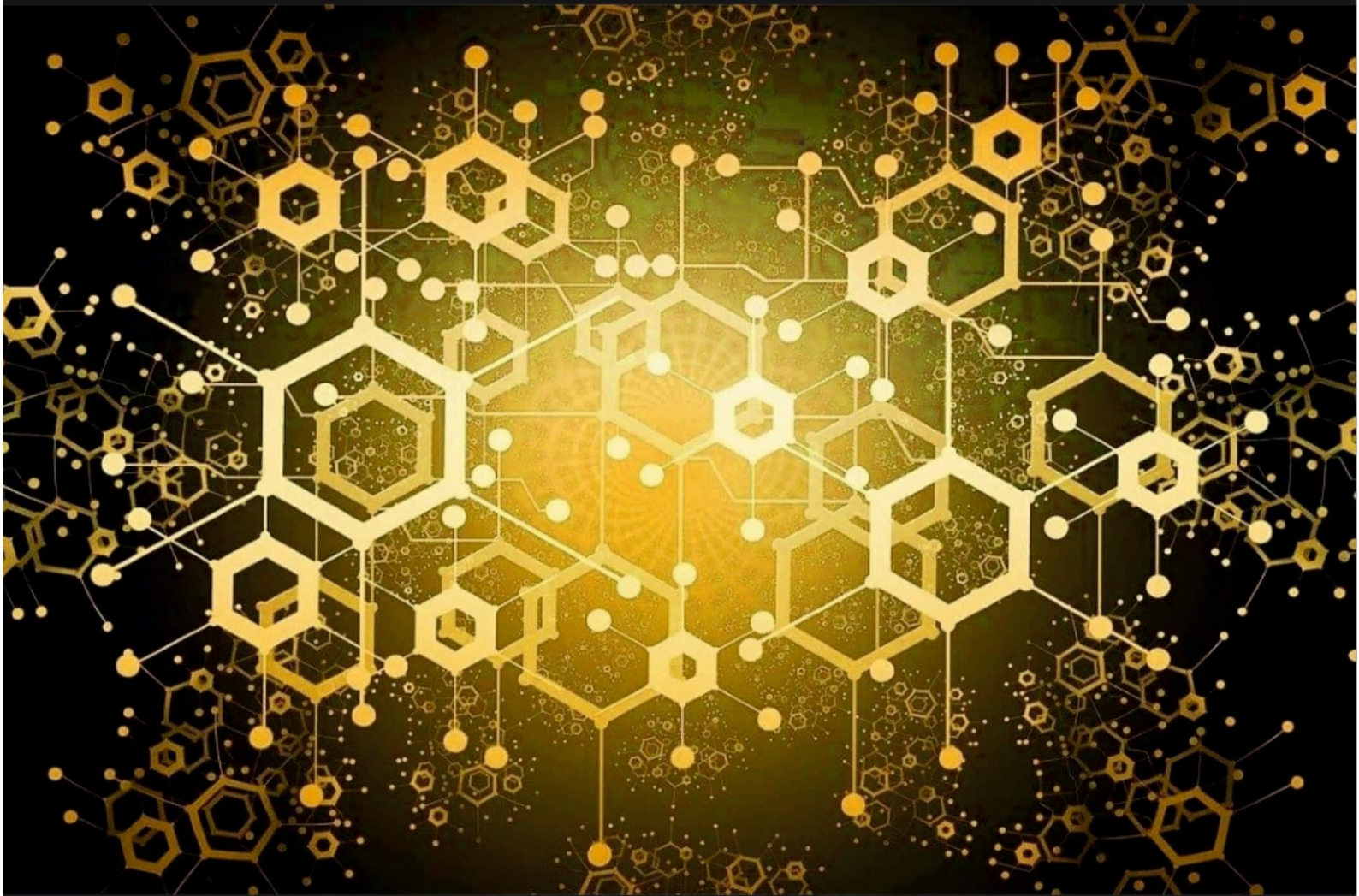


FUNDAMENTALS OF
BLOCKCHAIN
TECHNOLOGY



Dr. Sumangala Patil
Mukesh Bansal
Dr. Noorullah Shariff C.

Kripa Drishti Publications, Pune.

FUNDAMENTALS OF
BLOCKCHAIN
TECHNOLOGY

Dr. Sumangala Patil

Professor,

Computer Science & Engineering Department,
Faculty of Engineering & Technology (Co-Education) Sharanabasva
University, Kalaburagi, Karnataka.

Mukesh Bansal

Senior Director,

Head of CSP Sales,
MNC, UK.

Dr. Noorullah Shariff C.

Senior Professor,

Department of AI&ML,
Ballari Institute of Technology and Management,
Ballari.

Kripa-Drishti Publications, Pune.

Book Title: **Fundamentals of Blockchain Technology**

Authored By: **Dr. Sumangala Patil, Mukesh Bansal,
Dr. Noorullah Shariff C.**

Price: ₹599

1st Edition

ISBN: **978-81-19149-22-3**



Published: **April 2023**

Publisher:



Kripa-Drishti Publications

A/ 503, Poorva Height, SNO 148/1A/1/1A,
Sus Road, Pashan- 411021, Pune, Maharashtra, India.

Mob: +91-8007068686

Email: editor@kdpublications.in

Web: <https://www.kdpublications.in>

© Copyright Dr. Sumangala Patil, Mukesh Bansal, Dr. Noorullah Shariff C.

All Rights Reserved. No part of this publication can be stored in any retrieval system or reproduced in any form or by any means without the prior written permission of the publisher. Any person who does any unauthorized act in relation to this publication may be liable to criminal prosecution and civil claims for damages. [The responsibility for the facts stated, conclusions reached, etc., is entirely that of the author. The publisher is not responsible for them, whatsoever.]

PREFACE

The purpose of **Fundamentals of Blockchain Technology** book is to teach you about the theoretical aspects of blockchain technology. This book covers all the fundamentals of Blockchain technology that you need to know to become a Blockchain expert. This book is a vision to advance the technology behind this innovation, thus providing a fundamental explanation of this technology. With the help of this book, readers can learn the following topics in-depth in a very simple way: Introduction to Blockchain Cryptographic Primitives Blockchain Types Consensus Algorithms Challenges in Blockchain Technology.

This Book, equips you with an understanding of what blockchain is, how it works, and how it can enhance your business and the industry in which it operates. You learn the fundamentals of blockchain and how this technology will revolutionize transactions and business networks. You also discover the important difference between blockchain and block-chain for business and what makes blockchain an ideal solution for streamlining business networks. You will also discover Hyperledger, a Linux Foundation project, designed to help advance technology and thought leadership of cross-industry blockchain technologies. You learn about Hyperledger Fabric, an open source framework, and the instrumental role it plays in developing a blockchain for business. Finally, you find out everything you need to spin up a blockchain network today.

Abbreviations

Anti-Money Laundering (AML)

Application Binary Interface (ABI)

Bitcoin (BTC)

Bitcoin Cash (BCH)

Block Header (BH)

Byzantine Fault Tolerance (BFT)

Chain Virtual Machine (CVM),

Decentralised Applications (Dapps)

Decentralised Autonomous Organisations (DAOs)

Decentralized Autonomous Organization (DAO)

Denial of Service (DoS)

Digital Applications (DApps)

Directed Acyclic Graphs (DAG)

Distributed Denial of Service (DDoS)

Distributed Ledger Technologies (DLT)

Distributed Ledger Technology (DLT)

Domain Name System (DNS)

Domain Name System (DNS)

Ethereum Virtual computer (EVM)

Ethereum Virtual Machine (EVM)

Initial Coin Offerings (ICOs)

Initial Public Offering (IPO)

Internet of Things (IoT)

Know Your Customer (KYC)

Litecoin (LTC)

Machines as a Service (MaaS)

Man in The Middle (MITM)

Mobility Open Blockchain Initiative (MOBI)

Peer-To-Peer (P2P)

Progressive Web Apps (PWAs)

Proof of Activity (PoA)

Proof of Elapsed Time (PoET)

Proof of Stake (PoS)

Proof of Work (PoW)

Proof-Of-Work (PoW)

Pure Proof-Of-Stake (PPoS)

RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

Responsible Sourcing Blockchain Network (RSBN)

Self-Sovereign Identification (SSI)

Supply Chain Management (SCM)

USD Coin (USDC)

Verifiable Random Functions (VRF)

Virtual Machine (EVM)

Zero-Knowledge Proofs (ZKPs)

INDEX

Chapter 1: Introduction to Blockchain..... 1

1.1 Introduction:.....	1
1.2 History:	2
1.3 Blockchain Characteristics:.....	4
1.4 Distributed Ledger:.....	6
1.4.1 Distributed Ledger Technology (DLT):.....	7
1.4.2 Uses of Distributed Ledger Technology:	9
1.4.3 Advantages and Disadvantages of Distributed Ledger Technology: 10	
1.4.4 Types of Distributed Ledger Technology:.....	11
1.4.5 Below Are Some of the Types of DLT:	12
1.5 Distributed Ledgers Vs. Blockchain.....	14
1.6 Blockchain Categories:	14
1.6.1 Public Blockchain:	14
1.6.2 Private Blockchain:	17
1.6.3 Hybrid Blockchain:	18
1.6.4 Consortium Blockchain:.....	19
1.7 Blockchain Network and Nodes:.....	20
1.7.1 Peer-To-Peer Network:.....	20
1.8 Mining Mechanism:.....	26
1.9 Generic Elements of Blockchain:.....	27
1.10 Transferring Value Between Peers:.....	30
1.10.1 Immutable:.....	30
1.10.2 Distributed:	31
1.10.3 Decentralized:	32
1.10.4 Secure:	32
1.10.5 Consensus:	33
1.10.6 Unanimous:.....	33
1.10.7 Faster Settlement:.....	33
1.11 Permissioned Blockchain Network:	34
1.11.1 Industries That Benefit from Various Blockchain Networks:	35
1.12 Concerns Surrounding Blockchain Technology:	36

Chapter 2: Basic Distributed Computing & Crypto Primitives 37

2.1 Introduction:.....	37
2.2 Distributed System:	37
2.3 Distributed Computing:	40
2.4 Crypto Primitives:	41
2.5 Atomic Broadcast:	42

2.6 Consensus:	44
2.7 Byzantine Models of Fault Tolerance:	44
2.8 Hash Functions:.....	46
2.8.1 Puzzle Friendly Hash:	48
2.9 Digital Signatures:.....	49
2.10 Public Key Crypto:.....	52
2.10.1 Working On Public-Key Cryptography:	53
2.10.2 Benefits of Public-Key Cryptography:.....	54
2.11 Zero-Knowledge Systems:.....	57

Chapter 3: Blockchain Architecture.....60

3.1 Introduction:.....	60
3.2 Types of Blockchain Architecture Explained:	63
3.2.1 Public Blockchain:	64
3.2.2 Private Blockchain	65
3.2.3 Consortium Blockchain.....	66
3.3 Benefits of Blockchain:	69
3.4 Features of Blockchain Architecture:	69
3.4.1 Here the some of the features of Blockchain Architecture.....	69
3.5 Operation of Bitcoin Blockchain:	69
3.6 Bitcoin Blockchain Operations:	71
3.7 How to Invest in Bitcoin:.....	73
3.7.1 Bitcoin Cons:	73
3.8 Block:.....	73
3.8.1 Types of Blocks in Blockchain:.....	73
3.9 Hash:.....	74
3.9.1 Hashing used in Blockchain:	76
3.9.2 Types of Cryptographic Hash Functions:.....	77
3.9.3 Uses of Hash Functions in Blockchain:	79
3.10 Distributer P2P:.....	80
3.11 Structure of Blockchain:	82
3.12 Transaction State Machine:.....	83
3.12.1 Types of Accounts:	84
3.13 Delving into Block Structure:	85
3.14 Transactions:	86
3.14.1 Adding Transactions to a Block:.....	88
3.15 Appending Blocks to Blockchain:.....	89
3.16 Consensus Mechanism:.....	90
3.16.1 Future of Consensus Mechanisms:	90
3.16.2 Types of Consensus Mechanisms:	91

Chapter 4: Ethereum Basics98

4.1 Introduction:.....	98
4.2 Smart Contracts:.....	100

4.3 The Turing Completeness of Smart Contract:	103
4.3.1 The Turing Machine Leads to Turing Completeness:.....	103
4.3.2 Turing Completeness Applied to Blockchain Smart Contracts:	104
4.4 Smart Contract Languages and Verification Challenges:.....	107
4.4.1 The Main Smart Contract Challenges:	108
4.4.2 Legal Challenges:.....	109
4.4.3 Usability Challenges:	110
4.4.4 Impact Challenges:	111
4.5 Solving problems with Hedera:.....	111
4.6 Contracts to Enforce Legal Contracts:.....	111
4.6.1 Making Smart Contracts Enforceable:	112
4.6.2 Legal Challenges of Smart Contracts:.....	113
4.7 Smart Contracts the Future:	113
4.8 Comparing Bitcoin scripting vs. Ethereum Smart Contracts:.....	114
4.8.1 Bitcoin:	114
4.9 Ethereum:	114
4.9.1 Difference Between Bitcoin and Ethereum:	115
4.10 Scripting Language:.....	115
4.10.1 Costing:.....	115
4.10.2 Block limits:.....	116
4.10.3 Accounts:	116
4.10.4 Algorithm Performance:	116
4.10.5 Future Plans:	116
4.11 Bitcoin vs. Ethereum: Comparison Chart:	117
4.12 Writing Smart Contracts Using Solidity:.....	118
4.12.1 Solidity:	118
4.12.2 Contracts:.....	119
4.13 Initializing our Variables in Solidity Contracts and JavaScript:	120
4.13.1 Inheritance:	120
4.14 Solidity Functions:.....	121
4.15 JavaScript:	126

Chapter 5: Hyperledger Fabric 128

5.1 Introduction:.....	128
5.2 Hyperledger Fabric (A): Decomposing The Consensus Process:	131
5.2.1 How Does Hyperledger Fabric Work?.....	131
5.2.2 Hyperledger Fabric Consensus Algorithm:	133
5.2.3 Industry Use Cases for Hyperledger Fabric:	134
5.2.4 Benefits of Hyperledger Fabric:.....	135
5.2.5 Limitation of Hyperledger Fabric:	136
5.3 Hyperledger Fabric Components:.....	137
5.3.1 A Network Consists of:	138
5.3.2 Network Policies and Identities:	138
5.4 Chaincode Design and Implementation:.....	148
5.5 Chaincode in Hyperledger Fabric?.....	149

5.5.1 Types of Chaincodes in Hyperledger Fabric:.....	149
5.5.2 What Are System Chaincodes?	150
5.5.3 Chaincode for Developers in Blockchain:.....	151
5.5.4 Chaincode for Operators:	152
5.5.6 Beyond Chaincode:	153
5.5.7 Deploying A Chaincode:	153
5.5.8 Install and Define a Chaincode:.....	154
5.5.9 Upgrade A Chaincode:	163
5.5.10 Joining A Channel:.....	167
5.6 Fabric SDK and Front End:	173
5.6.1 Methods in Fabric-Network:	175
5.7 Hyperledger Composer Tool:.....	176
5.7.1 Key Concepts in Hyperledger Composer:.....	177
5.7.2 Architecture of Hyperledger Composer:	178
5.7.3 Hyperledger Composer Working:.....	180
Chapter 6: Blockchain Use Cases	181
6.1 Introduction:.....	181
6.2 Blockchain Technology Use Cases	182
6.2.1 Smart Contracts:	182
6.2.2 Internet of Things (IoT):.....	183
6.2.3 Money Transfer:	184
6.2.4 Personal Identity Security:	184
6.2.5 Logistics:	186
6.2.6 Digital Media:	187
6.2.7 Education:.....	187
6.2.8 Medical Field:.....	188
6.2.9 Entertainment:.....	189
6.2.10 Real Estate:	189
6.3 Blockchain in Supply Chain:	190
6.3.1 Blockchain Provide Supply Chain Solutions:	194
6.3.2 Blockchain in Supply Chain Use Cases	196
6.4 Blockchain in Manufacturing:	197
6.4.1 Benefits of Using Blockchain in Manufacturing:.....	198
6.5 BCG: Five Ways Blockchain Can Create Value In The Factory Of The Future	200
6.5.1 Enhancing Track and Trace:.....	200
6.5.2 Protecting and Monetising Critical Intellectual Property:.....	200
6.5.3 Simplifying and Safeguarding Quality Checks:	201
6.5.4 Advancing Machines as A Service:	201
6.5.5 Enabling Machine-Controlled Maintenance:.....	202
6.6 Blockchain in Automobiles:	203
6.6.1 Bolstering Supply Chain Management:	204
6.6.2 Cutting Costs:	204
6.6.3 Improving End User Experience:	205

6.6.4 Providing The Backbone of an Ecosystem of Autonomous Vehicles:	205
6.7 Blockchain Be Implemented in The Automotive Industry:	206
6.7.1 Ensuring Ethical Sourcing of Raw Materials:	206
6.7.2 Digital Passports for Vehicles:	207
6.7.3 Ride and Car Sharing Apps:	207
6.7.4 Platforms for Autonomous Vehicle Fleet Management:	208
6.8 Blockchain in Healthcare:	208
6.8.1 Blockchain and Healthcare Data Security:	209
6.8.2 Blockchain Medical Records:	211
6.8.3 5 Blockchain Healthcare Use Cases in Digital Health:	215
6.9 Blockchain in Cyber Security:	222
6.9.1 Possible Blockchain Use Cases for Cybersecurity	223
6.9.2 Application of Blockchain in Cybersecurity:	224
6.9.3 Cons of Using Blockchain in Cybersecurity:	225
6.10 Blockchain in Financial Industry:	227
6.10.1 Blockchain in Finance Examples:	227
6.11 Security and Transparency:	230
6.11.1 Reduced Costs:	231
6.11.2 Effectively Control Risks:	231
6.11.3 Instant Settlements:	232
6.11.4 Better Auditing:	233

Chapter 7: Privacy, Security Issues in Blockchain 239

7.1 Introduction:	239
7.2 Blockchain and Privacy Protection:	240
7.2.1 Private and Public Keys:	240
7.2.2 Peer-To-Peer Network:	241
7.2.3 Blockchain Security:	243
7.3 Zcash:	246
7.3.1 Zcash Transaction Types:	246
7.3.2 Future of Zero-Knowledge Proofs:	247
7.3.3 Zk-SNARKS for Anonymity Preservation:	247
7.3.4 Zero-Knowledge Proof	248
7.3.5 Criticism of zk-SNARKs	249
7.4 Attacks on Blockchain:	250
7.4.1 51% Attack:	250
7.4.2 Eclipse Attack:	251
7.4.3 Sybil Attack:	252
7.4.4 Timejacking Attack:	253
7.4.5 Selfish Mining Attack:	253
7.4.6 Finney Attack:	254
7.4.7 Race Attack:	254
7.5 Advent of Algorand:	255
7.5.1 Algorand Protocol Structure:	256

7.5.2 Algorand Staking Mechanism: Pure Proof-Of-Stake.....	256
7.5.3 Production of Algorand Blocks Under Ppos:	257
7.5.4 Algorand’s Native Cryptocurrency: ALGO	258
7.6 Sharding Based Consensus Algorithms to Prevent These Attacks:	259
7.7 Blockchain Nodes:	259
7.8 Horizontal Partitioning:	260
7.9 Shard Sharing:.....	260
7.9.1 Sharding and Security:	261
8. References.....	262

ABOUT THE EDITORS



Dr. Sumangala Patil (B.E., M.Tech., Ph.D., MISTE)

Currently working as a Professor in Computer Science & Engineering Department, Faculty of Engineering & Technology (Co-Education) Sharanabasva University, Kalaburagi, Karnataka State
Former Associate Professor @ Lingaraj Appa Engineering College, Bidar.
Former Associate Professor @ PVKK Institute of Technology, Ananthapur.
Attended number of Faculty Development Program & Workshop.
Number of Workshops & Conferences are Organized

BE (E&CE) First Class passed out year 1993,

M.Tech (Computer Science & Engineering) First Class passed out year 2001.

Ph D in (Computer Science & Engineering) Awarded 2020, from JNT University Ananthapur (AP).

12 No of National & International Journal Research Paper are published.

Recognized by the Visvesvaraya Technological University, Belagavi for Ph.D. Recognized Guide.

Total Teaching Experience is more than 25 years.



Mukesh Bansal (B.E., MS, pursuing PhD)

Currently working as senior director in Europe based MNC, he is an experienced I.T. / Telecommunication professional and executive with broad and well-balanced technical, commercial, business and people management skills. Former scientist in ISRO, and town councilor of Newbury (UK) Town Council, he has vast experience in the telecommunications and research industries managing complex transformational deals and advising clients on various strategic issues. He has authored various research and white papers in area of intelligent OSS, blockchain and Network Security domains. He is MSP, PRINCE2, ITIL, PRINCE2 Agile, CEH, CISM, CISO certified and holds bachelor's degree from Engineering College Kota, Master's degree from BITS PILANI and currently pursuing PhD in cyber security.



Dr. Noorullah Shariff C. received the B.Tech (ECE) degree from NITK, Surathkal in 1984, ME (Guided Missiles) from DIAT, Pune in 1986 and PhD(CSE) Degree from Monad University, Hapur in 2013. He is currently a Senior Professor at the Department of AI&ML, Ballari Institute of Technology and Management, Ballari. He has worked as Professor, HOD, Vice Principal (Academics) & Principal in various Engineering colleges with a total experience of 36 years. He has 30 research papers in national and international conferences and journals to his credit. He has conducted national and international conferences, FDP and workshops.



Kripa-Drishti Publications
A-503 Poorva Heights, Pashan-Sus Road, Near Sai Chowk,
Pune - 411021, Maharashtra, India.
Mob: +91 8007068686
Email: editor@kdpublishations.in
Web: <https://www.kdpublishations.in>

Price: ₹ 599

ISBN: 978-81-19149-22-3

