

Blockchain and DLT

*A comprehensive guide to getting started
with Blockchain and Web3*

Nakul Shah



www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

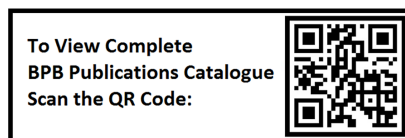
ISBN: 978-93-55519-283

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.



Dedicated to

To my Mom (Shalini Shah),

Dad (Satish Shah)

and

Wife (Mauli Shah)

About the Author

Nakul Shah, a seasoned professional with over nine years of experience in the software industry, currently serves as a subject matter expert in the emerging technology space. Holding a Master's degree in Financial Engineering from the University of Michigan, Nakul combines academic prowess with extensive practical knowledge.

Nakul's expertise lies in product development and technical content creation. A certificate in Blockchain and Crypto attests to his commitment to staying at the front of advancements in the field.

Nakul is an industry thought leader who authored the book *Blockchain for Business with Hyperledger Fabric*. He is proficient in explaining complex concepts and making them accessible to a broad audience. Nakul actively participates in affiliations and collaborations within the technology community, and conferences across the globe.

With a solid educational foundation, rich professional experience, and a commitment to ongoing learning, Nakul Shah continues to shape the landscape of blockchain technology, offering valuable insights and expertise to the global community.

About the Reviewer

Pradeep Selvaraj, a master in the domain of 3D web development, Metaverse innovation, AI Apps, Blockchain, and NFT development. He brings over 15 years of rich experience in the IT sector. He boasts an impressive array of certifications, including being a Google certified TensorFlow Developer, a certified blockchain developer from the Blockchain Council, and a Data Alchemist accredited by Covalent.

In addition to his reviewer role, he is the CEO and founder of Leogacy, a pioneer in AI SaaS, Metaverse, and 3D AR/VR initiatives. Under his visionary leadership, **Leogacy** has launched the NFT project '8lements'. His multifaceted expertise ensures a comprehensive and insightful review, enriching the reader's understanding of the dynamic world of blockchain and AI.

Our reviewer's expertise extends to offering nuanced, in-depth analyses of blockchain and AI, making his perspectives invaluable for both veterans and novices in these fields. He is at the forefront of pioneering work, currently dedicated to developing 3D Animated NFTs in the Metaverse named Diamond Floaters.

Acknowledgement

I extend my sincere appreciation to three key individuals who played crucial roles in the process of crafting this book—my parents and my wife.

To my parents, *Shalini Shah and Satish Shah*, your continuous support and confidence in me have been a driving force. Your belief in my pursuits has provided the confidence needed to navigate the complexities of this project and life. Your support is the foundation upon which my work stands, and for that I am sincerely grateful.

To my wife, *Mauli Shah*, your patience and consistent encouragement have been invaluable. Your belief in my abilities, and the time you dedicated to supporting my endeavors have contributed immensely to all my endeavors. Your support has provided stability throughout the challenges and triumphs of this process.

I express my deep gratitude to my family for their understanding and shared moments of joy. Your collective support has been an essential component in the development of this book.

To Mom, Dad, and *Mauli*, this book reflects on the impact of your support. I appreciate your crucial roles in this journey, and I thank you for being integral to the realization of this endeavor.

Preface

Blockchain is a transformative force, reshaping several industries and technologies and redefining data integrity. This book is designed to be your guide by providing a comprehensive explanation for engineering students and enthusiasts. It simplifies the complex concept of blockchain and **Distributed Ledger Technology (DLT)**.

In this book, you will learn about many topics, from the basics of blockchain and DLT to the real-world application of blockchain. You will also learn about Bitcoin, permissionless and permissioned blockchain, and will be provided with numerous practical examples to help you understand the concepts.

I hope you will find this book informative and helpful when unraveling the foundations of decentralized systems and exploring the limitless potential of blockchain.

Chapter 1: Cryptography and Distributed Systems – In this chapter, the focus is on the intersection of cryptography and distributed systems. The chapter begins by introducing the fundamental concepts of both cryptography and distributed systems, highlighting their importance in securing and managing data in a networked environment. It explores concepts like public-key cryptography, digital signatures, and secure multi-party computation are explored in the context of distributed systems. The chapter also explores the implementation of cryptographic primitives in blockchain technology and other distributed ledger systems. The importance of cryptographic algorithms in achieving consensus mechanisms, like proof-of-work or proof-of-stake, is also discussed.

Chapter 2: Introduction to Blockchain Technology – This chapter addresses the technical intricacies of blockchain technology and DLT. It also explores key theoretical aspects such as the CAP theorem, the Byzantine Generals Problem, and the nuances of consensus mechanisms, including types, cryptographic primitives, and data structures underpinning blockchain functionality.

Chapter 3: Bitcoin – This chapter discusses Bitcoin, covering its historical genesis, transaction dynamics, and foundational concepts. It also explores Bitcoin keys, addresses, and wallets, including elliptic curve cryptography, Base58 encoding, and BIP-38 encryption. In this chapter you will learn about transaction scripts, mining intricacies, and the structure of blocks, culminating in the pivotal genesis block. It will help you navigate the Bitcoin network, addressing core nodes, peer-to-peer architecture, and incentive-based

engineering. The chapter concludes by exploring Bitcoin forensics, analyzing addresses and wallets precisely.

Chapter 4: Permissionless Blockchain: Ethereum – This chapter introduces Ethereum 1.0 and 2.0 and gives a detailed exploration of the Turing completeness inherent in the **Ethereum Virtual Machine (EVM)**, and a meticulous comparison with Bitcoin. The discourse extends to practical aspects such as Ether units, Ethereum wallets, and the utilization of Metamask. Transactional intricacies are examined, including structure, gas dynamics, and the conveyance of values to **Externally Owned Accounts (EOA)** and Contracts. The chapter culminates with a formal discussion on Smart Contracts and their deployment through Solidity.

Chapter 5: Permissioned Blockchain: Hyperledger Fabric – This chapter focuses on Hyperledger Fabric and encompasses an in-depth introduction to the framework, elucidating the tools and architecture integral to Hyperledger Fabric Blockchain. The chapter further delves into the intricate components of Hyperledger Fabric while addressing challenges related to interoperability and scalability within the blockchain landscape.

Chapter 6: Crypto Assets and Cryptocurrencies – This chapter dissects concepts like ERC20 and ERC721 Tokens, exploring the differences between ERC-721 and ERC-20 tokens, and talks about the significance of **Non-Fungible Tokens (NFT)**. This chapter serves as a guide to navigating complex digital assets and provides a great understanding of **Initial Coin Offerings (ICO)**, **Security Token Offerings (STO)**, and diverse cryptocurrencies.

Chapter 7: Blockchain Applications and Case Studies – This chapter introduces readers to the transformative impact of blockchain in IoT, AI, and cyber security. Explore how blockchain enhances security in the Internet of Things, ensures ethical AI applications, and fortifies cyber defenses. Real-world case studies exemplify the practical implications, making this chapter an essential guide to the evolving intersection of blockchain technology and these dynamic domains.

Code Bundle and Coloured Images

Please follow the link to download the *Code Bundle* and the *Coloured Images* of the book:

<https://rebrand.ly/er2r3cg>

The code bundle for the book is also hosted on GitHub at

<https://github.com/bpbpublications/Blockchain-and-DLT>.

In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **<https://github.com/bpbpublications>**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at business@bpbonline.com with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit www.bpbonline.com. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit www.bpbonline.com.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

<https://discord.bpbonline.com>



Table of Contents

1. Cryptography and Distributed Systems	1
Introduction	1
Structure	1
Objectives	2
Routes of cryptography.....	2
<i>Monoalphabetic cipher</i>	3
<i>Polyalphabetic cipher</i>	3
<i>Egyptians</i>	4
<i>Greeks</i>	4
Emergence of distributed system	4
<i>Edge computing</i>	6
Cryptography's basic concepts and terminologies	8
<i>Know about cryptography</i>	9
<i>Encryption: A way to secure system</i>	10
<i>Industrial impact of cryptography</i>	12
Evolution of cryptography	12
<i>Public key cryptography</i>	13
<i>RSA algorithm</i>	13
<i>Elliptic curve cryptography</i>	14
<i>Key generation</i>	14
<i>Digital signatures</i>	14
<i>Implementation note</i>	15
Encryption.....	15
<i>Secure communication</i>	16
Principles of cryptography	17
Encryption algorithms.....	18
<i>Symmetric-key encryption</i>	18
<i>Data encryption standard</i>	18
<i>Advanced encryption standard</i>	19

Working of Diffie-Hellman	20
Limitations of Diffie-Hellman.....	24
Application of symmetric encryption.....	25
Pros and limitations of symmetric encryption	25
Asymmetric-key encryption.....	25
The functionality of asymmetric encryption.....	27
Different types of asymmetric encryption algorithms	28
Pros and cons of asymmetric encryption	29
Pros.....	29
Cons.....	29
Cryptographic protocols.....	31
Cryptographic key management.....	32
Process of cryptographic key management	32
Public key cryptography.....	33
Principles behind public key cryptography.....	33
Public key cryptosystem applications.....	34
RSA	35
El Gamal cryptography algorithm	36
Elliptic Curve Cryptography.....	36
Hash functions.....	37
The inner workings of hashing algorithms	38
Common cryptocurrency hash functions.....	39
Digital signature.....	39
Fundamentals of distributed systems	40
Understanding popular consensus mechanisms	42
Distributed file systems.....	44
Features of distributed file system.....	45
Distributed database.....	46
Different types of Distributed databases.....	47
Distributed database features.....	49
Distributed database types.....	50
Blockchain and cryptography integration.....	51

<i>Public and private key system</i>	52
<i>Bitcoin network: Proof of work</i>	52
Ethereum network: Proof of stake	52
<i>Applications of blockchain technology</i>	53
<i>Smart contracts</i>	54
<i>Different models of smart legal contracts</i>	54
<i>External</i>	54
<i>Internal</i>	55
<i>Distributed ledger technology</i>	55
Impact of cryptography blockchain	56
<i>Understanding blockchain cryptography</i>	56
<i>Network security</i>	57
<i>Intrusion detection and prevention system</i>	58
<i>Types of intrusion detection and prevention systems (IDPS)</i>	60
Security protocols.....	60
<i>Security standards</i>	61
Conclusion	64
Question and answers	65
Multiple choice questions	65
<i>Answers</i>	66
2. Introduction to Blockchain Technology	67
Introduction	67
Structure	68
Objectives	68
Rise of blockchain technology.....	68
<i>Defining blockchain</i>	69
<i>Problems with a centralized system</i>	70
<i>Centralized vs. decentralized vs. distributed architecture</i>	71
<i>Blockchain: A comprehensive network architecture</i>	74
<i>Simplified architecture of blockchain</i>	77
<i>Key characteristics of blockchain architecture</i>	78
Technical definition of a blockchain.....	80

<i>Understanding blockchain ledgers</i>	82
<i>Blockchain events</i>	86
<i>Features of blockchain</i>	86
<i>Decentralization</i>	87
<i>Immutable</i>	87
<i>Efficient</i>	88
<i>Enhanced security</i>	88
<i>Transparent</i>	89
Different types of blockchain.....	89
<i>Public blockchains</i>	90
<i>Private blockchains</i>	91
<i>Consortium blockchains</i>	91
<i>Hybrid blockchain</i>	93
Distributed ledger technology versus blockchain.....	94
<i>CAP theorem</i>	95
Byzantine generals problem.....	96
Consensus mechanism.....	98
Cryptographic primitives.....	100
Data structure used in blockchain.....	101
<i>Relevance of block in blockchain</i>	101
<i>Features of a block</i>	103
<i>Block header</i>	104
Block header hash and block height.....	104
<i>Genesis block</i>	105
<i>Linking blocks in the blockchain</i>	106
<i>Merkle tree</i>	106
Conclusion.....	110
Questions and answers.....	110
Multiple choice question.....	111
<i>Answers</i>	112
3. Bitcoin	113
Introduction.....	113

Structure	114
Objectives	114
Bitcoin	114
<i>Basics of Bitcoin</i>	115
<i>History of Bitcoin</i>	117
<i>Bitcoin transaction</i>	118
<i>Bitcoin concepts</i>	119
<i>Key</i>	120
<i>Address</i>	120
<i>Wallet</i>	120
<i>Bitcoin transaction</i>	120
<i>Unspent transaction outputs</i>	120
Validation of transaction.....	121
Consensus mechanism	123
<i>Bitcoin keys</i>	124
<i>Securing private keys in blockchain</i>	126
<i>Elliptic curve cryptography</i>	128
<i>Bitcoin address</i>	131
<i>Base58</i>	132
<i>Utility of Base58</i>	133
<i>Encoding with Base58</i>	134
<i>Base58 decoding process</i>	136
Encrypted private keys	137
Pay-to-script address	138
Multi-sig addresses	140
<i>Working of multi-sign addresses</i>	140
<i>Benefits of multi-signature addresses</i>	142
<i>Examples of multi-signature address use</i>	142
<i>Cold storage</i>	142
<i>Escrow services</i>	143
Vanity address	143
Bitcoin wallet	144

<i>Bitcoin HD wallet</i>	146
<i>Creating an HD wallet from the seed</i>	148
<i>Derive private child key</i>	148
<i>Derive public child key</i>	149
Transaction script	150
<i>Script address</i>	152
Bitcoin mining	154
<i>History of Bitcoin mining</i>	155
<i>Working of bitcoin mining</i>	155
Structure of a block	159
<i>Block header</i>	160
<i>Genesis block</i>	162
<i>Linking of blocks</i>	163
Type of full nodes.....	165
<i>Bitcoin core application programming interface</i>	166
Peer-to-peer network.....	166
Nodes and roles involved.....	168
Incentive based engineering.....	170
Extended bitcoin network.....	171
Bitcoin relay network	172
Network discovery	172
<i>Full node</i>	173
<i>Exchange network</i>	174
<i>Nodes communication</i>	175
<i>Simplified payment verification</i>	175
<i>SPV nodes and privacy</i>	176
<i>Transaction pool</i>	176
<i>Blockchain fork</i>	177
<i>Bitcoin testnet</i>	178
Basics of Bitcoin forensic.....	178
Clustering of address.....	179
Conclusion	180

Questions and answers	180
Multiple choice questions	181
<i>Answers</i>	182
4. Permissionless Blockchain: Ethereum	183
Introduction	183
Structure	183
Objectives	184
Introducing Ethereum	184
<i>Turing completeness</i>	185
<i>Use cases and real-world applications</i>	186
Understanding Ethereum 1.0 and 2.0	186
<i>Ethereum 1.0: Creating decentralized ecosystems</i>	187
<i>Ethereum 2.0: Bringing scalability and efficiency</i>	188
Beacon Chain	189
The shard chains: Scaling Ethereum	189
Ethereum virtual machine	190
<i>Role of EVM</i>	191
<i>Stack based architecture of EVM</i>	192
Smart contracts and gas	193
<i>Gas: Efficient execution on the EVM</i>	194
Comparing Bitcoin and Ethereum.....	195
<i>Purpose and functionality</i>	195
<i>Blockchain architecture</i>	196
<i>Tokenomics</i>	196
<i>Developer community and ecosystem</i>	197
Types of accounts in Ethereum	198
<i>Real-world examples</i>	204
Contract transactions on Ethereum	205
<i>Structure of transaction</i>	206
<i>Transaction flow</i>	207
<i>Transaction nonce</i>	207
<i>Nonce generation and sequential ordering</i>	208

<i>Definition and importance of transaction gas</i>	209
<i>Gas price and gas limit</i>	209
<i>Impact on transaction confirmation</i>	209
<i>Gas fee calculation</i>	210
<i>Factors affecting transaction gas calculation</i>	210
<i>Gas limit and out-of-gas errors</i>	210
<i>Practical examples of gas usage</i>	211
<i>Gas optimization</i>	211
<i>Transaction recipient</i>	211
<i>Transaction values and data</i>	212
<i>Transaction values</i>	212
<i>Transaction data</i>	213
<i>Transaction values to EOA and contracts in Ethereum</i>	214
Smart contracts and Solidity.....	215
<i>Solidity: The language of smart contracts</i>	216
<i>Solidity development tools</i>	216
<i>Best practices and considerations</i>	216
<i>Development environment and client</i>	217
<i>Development environment</i>	217
<i>Client software</i>	217
Basics of Solidity.....	218
<i>Solidity development process</i>	219
<i>Pros and cons of Solidity</i>	219
<i>Life cycle of a smart contract</i>	220
<i>Smart contract programming using Solidity</i>	221
<i>Reentrancy in Solidity</i>	225
<i>Upgradeability of smart contracts</i>	226
Introduction to MetaMask.....	227
<i>Working principles of MetaMask</i>	229
<i>Use cases of smart contracts</i>	229
<i>Opportunity and risks of smart contract</i>	231
<i>Smart contract deployment</i>	233

Truffle: Smart contract development.....	235
<i>Significance of Truffle in smart contract development.....</i>	236
Remix and test networks.....	238
<i>Remix: An accessible IDE.....</i>	238
<i>Importing from GitHub.....</i>	239
<i>Plugin management.....</i>	239
<i>Deployment on testnets.....</i>	239
<i>Additional features.....</i>	240
<i>Test networks: Simulating blockchains.....</i>	240
Conclusion.....	241
Questions and answers.....	241
Multiple choice questions.....	242
<i>Answer.....</i>	243
5. Permitted Blockchain: Hyperledger Fabric.....	245
Introduction.....	245
Structure.....	246
Objectives.....	246
Defining permitted blockchains.....	247
<i>Architecture of permitted blockchains.....</i>	247
<i>Use cases and applications.....</i>	248
Architecture of Hyperledger Fabric.....	249
<i>The modular design.....</i>	249
<i>Why Hyperledger Fabric.....</i>	250
Chaincode.....	252
<i>Lifecycle of a chaincode.....</i>	253
<i>Transaction processing.....</i>	254
<i>Upgrading.....</i>	254
<i>Maintenance.....</i>	255
<i>Scaling.....</i>	255
The ordering services.....	255
Membership services.....	255
<i>Real-world deployments.....</i>	256

Hyperledger project: Framework	256
<i>Collaborative innovation</i>	256
<i>Open-source philosophy</i>	256
<i>Hyperledger greenhouse</i>	257
<i>Practical applications</i>	257
<i>Down to earth approach</i>	257
Structure of Hyperledger	257
<i>Hyperledger umbrella</i>	258
<i>Hyperledger projects</i>	258
<i>Diverse contributions</i>	258
<i>Hyperledger Fabric V1 architecture</i>	258
<i>Network components</i>	259
<i>Smart contracts and ledgers</i>	259
<i>Channels for privacy</i>	260
<i>Consensus mechanisms</i>	260
Introduction to Hyperledger Sawtooth	260
<i>Modularity and components</i>	261
<i>Hyperledger Sawtooth architecture</i>	261
<i>Features and benefits</i>	261
<i>Real-world applications</i>	262
Introduction to Hyperledger Iroha	262
<i>Core components of Hyperledger Iroha</i>	263
<i>Hyperledger Iroha features</i>	264
<i>Real-world applications of Hyperledger Iroha</i>	264
Introduction to Hyperledger Burrow	264
<i>EVM connection</i>	265
<i>Real-world applications</i>	265
Hyperledger Indy: Disrupting digital identity	266
<i>Hyperledger Indy components</i>	266
<i>Real-world applications</i>	267
Hyperledger ecosystem	267
<i>Hyperledger Fabric</i>	267

<i>Hyperledger Sawtooth</i>	267
<i>Hyperledger Indy</i>	267
<i>Hyperledger Besu</i>	268
<i>Hyperledger Burrow</i>	268
<i>Hyperledger Aries</i>	268
Hyperledger tooling and utility libraries	268
<i>Composer: A tool for rapid development</i>	268
<i>Caliper: Benchmarking and performance testing</i>	269
<i>Explorer: Visualizing the blockchain</i>	269
<i>Quilt: Enabling interledger payments</i>	269
<i>Ursa: A crypto-library repository</i>	269
<i>Other utility libraries</i>	269
Blueprint of Hyperledger Fabric.....	270
<i>Endorsement and validation</i>	270
<i>Modular and pluggable design</i>	271
<i>Real-world applications</i>	271
<i>Components of Hyperledger Fabric</i>	272
<i>Peer nodes: The workhorses of the network</i>	272
<i>Ordering service: Orchestrating the transaction flow</i>	272
<i>Membership services: The gatekeepers</i>	272
<i>Ledger: Recording the immutable history</i>	272
<i>Smart contracts</i>	272
<i>Channels for privacy</i>	273
<i>Consensus mechanisms</i>	273
MSPs: The guardians of identity.....	273
<i>Role of MSPs</i>	273
<i>MSP configuration in Fabric</i>	274
Chaincode	274
<i>Components of MSPs</i>	278
<i>Security considerations while configuring MSP</i>	278
<i>MSPs in action</i>	279
<i>Certificate authority</i>	280

<i>Certificate hierarchy</i>	280
<i>Use cases</i>	281
Nodes: The building blocks.....	281
<i>Node hierarchy</i>	282
<i>Real-world applications</i>	283
Chaincode: The logic of transactions	283
<i>Programming languages for chaincode</i>	284
<i>Real-world applications</i>	284
Channels: Enabling privacy and segmentation.....	285
<i>Creating and managing channels</i>	286
<i>Real-world applications</i>	286
Consensus mechanisms in Hyperledger Fabric	286
<i>Solo consensus: The lone decision maker</i>	286
<i>Kafka consensus: Distributed decision making</i>	287
<i>Raft consensus: A leader-follower model</i>	287
<i>Real-world applications</i>	287
Interoperability and scalability	288
<i>Interoperability: Bridging the blockchain divide</i>	288
<i>Challenges of interoperability</i>	288
<i>Scalability: Handling the growing load</i>	289
<i>Improving channels' efficiency</i>	289
<i>Considerations for consensus mechanisms</i>	291
<i>Strategies and solutions</i>	292
Conclusion	292
References	292
Questions and answers	292
Multiple choice questions.....	293
<i>Answers</i>	294
6. Crypto Assets and Cryptocurrencies	295
Introduction	295
Structure	296
Objectives	296

ERC-20, ERC-721, and ERC-1155 tokens	296
<i>ERC-20 tokens: The fungible tokens</i>	296
<i>The anatomy of ERC-20 tokens</i>	297
<i>Use cases and real-world applications of ERC-20 tokens</i>	297
<i>ERC-721 tokens: The non-fungible tokens</i>	297
<i>Understanding ERC-721 tokens</i>	298
<i>Applications and creative possibilities of ERC-721 tokens</i>	298
<i>ERC-1155 tokens: A multi-token standard</i>	299
<i>Highlights of ERC-1155 tokens</i>	299
<i>Use cases of ERC-1155 tokens</i>	299
Defining a token	299
ERC: A set of standards	300
Fungible vs. Non-fungible tokens	300
<i>Fungible tokens</i>	300
<i>NFTs</i>	301
<i>Difference between ERC-721, ERC-20, and ERC-1155 tokens</i>	302
Exploring NFTs	303
<i>Working of NFTs</i>	304
<i>Examples of NFTs</i>	304
<i>Usage of NFTs</i>	305
<i>Difference between NFTs and other cryptocurrencies</i>	305
NFT marketplaces	305
Introducing initial coin offerings	306
<i>Functioning of the ICO mechanism</i>	306
<i>ICOs and liquidity pool</i>	308
<i>Decoding crypto exchanges</i>	308
<i>Binance</i>	308
<i>Uniswap</i>	308
Security token offerings	309
Diverse cryptocurrency landscape	310
Cryptocurrencies in everyday life	311
Conclusion	311

Questions and answers	311
Multiple choice questions	312
<i>Answers</i>	313
7. Blockchain Applications and Case Studies.....	315
Introduction	315
Structure	315
Objectives	316
Blockchain in IoT.....	316
<i>Understanding IoT and its challenges</i>	316
<i>Blockchain and IoT together</i>	317
<i>Real-world implementations</i>	317
Blockchain with artificial intelligence	318
<i>AI in blockchain governance models</i>	318
<i>Benefits of AI's predictive analysis</i>	318
<i>Challenges in collaboration of blockchain and AI</i>	319
<i>The blockchain solution</i>	319
<i>Real-world applications</i>	319
<i>The future of blockchain in AI</i>	320
Blockchain improving cybersecurity.....	320
<i>Understanding the threat landscape</i>	320
<i>Blockchain's defensive arsenal</i>	321
<i>Real-world applications</i>	321
<i>The future of blockchain in cybersecurity</i>	322
Conclusion	322
Questions and answers	323
Multiple choice questions	323
<i>Answers</i>	324
Index.....	325-335

CHAPTER 1

Cryptography and Distributed Systems

Introduction

Cryptography and distributed systems have emerged as the primary disciplines in the field of modern data security and efficient information exchange. Cryptography symbolizes the centuries-old quest for secure communication. Cryptography has transcended boundaries, from the cryptic hieroglyphs to the complex algorithms of the contemporary time. Meanwhile, the concept of distributed systems has germinated from the continuous evolution of computing and networked systems and aims to transform the way data is accessed, shared, and utilized across various platforms through collaborative data sharing, processing, and scalability.

This chapter will explore the intertwined disciplines of cryptography and distributed systems. Besides the histories and complexities of these groundbreaking technologies, we will learn about the nuances of encryption, digital signatures, key exchange, authentication mechanisms, and more.

Structure

This chapter contains the following topic:

- Routes of cryptography

- Emergence of distributed system
- Cryptography's basic concepts and terminologies
- Evolution of cryptography
- Encryption
- Principles of cryptography
- Encryption algorithms
- Working of Diffie-Hellman
- Cryptographic protocols
- Cryptographic key management
- Public key cryptography
- Hash functions
- Distributed file systems
- Distributed database
- Blockchain and cryptography
- Security protocols

Objectives

The chapter elucidates the interrelated relationship between cryptography and distributed systems and how their integration strengthens the security and integrity of decentralized networks. It aims to offer a comprehensive understanding of cryptography and distributed systems by shedding light on their evolution, fundamentals, features, and applications. The chapter will talk about encryption algorithms, encryption standards, cryptographic protocols, and more in detail. Through this, we will gain insights into their collaborative potential in addressing the technological challenges of contemporary times.

Routes of cryptography

Trails of cryptography trace way back in time, when simpler methods of encryptions were used, such as transposition ciphers, and polyalphabetic ciphers for high termed security contents. Encrypting things was fun during the childhood days for most of us, as we used to swap messages to our best buddies. Everyone might have used one or the other way to hide the message content from public like the use of invincible ink or wax. The necessity to hide messages has been present since we transitioned from living in caves to forming communities and embracing the concept of civilization. Once distinct groups or tribes emerged, the notion of competing against each other arose and was disseminated, accompanied by hierarchical aggression, covert communication, and manipulation of

the masses. The most primitive forms of encryption were discovered in the birthplace of civilization, which is unsurprising, encompassing areas presently associated with Egypt, Greece, and Rome.

The earliest known form of cryptography dates back to ancient Egypt, where hieroglyphs were used to encrypt sensitive information. Throughout history, various forms of cryptography have been used, including substitution ciphers, transposition ciphers, and polyalphabetic ciphers.

The Caesar cipher, named after Julius Caesar (a Roman military general in 100BCE) who used it to encrypt his military messages, is one of the simplest and earliest known substitution ciphers. The Vigenère cipher and the Playfair cipher, developed in the 16th and 19th centuries respectively, are examples of polyalphabetic ciphers. These traditional methods of encryption can easily be broken by modern computers and are no longer considered secure for protecting sensitive information.

Monoalphabetic and polyalphabetic ciphers are two types of secret codes used in cryptography.

Monoalphabetic cipher

In a monoalphabetic cipher, each letter in a message is consistently replaced with a single, fixed letter. For instance, in a Caesar cipher, every *A* might always become a *G*, leading to a simple and predictable substitution. However, monoalphabetic ciphers are vulnerable to attacks like frequency analysis, where the frequency of letters in the encrypted message is analyzed to crack the code.

In this cipher, each letter in the plaintext is shifted by a fixed number of positions in the alphabet.

For instance, with a shift of 3, the following changes can be observed:

- **Original:** HELLO
- **Encrypted:** KHOOR

Here, each letter is replaced by the letter that is three positions ahead in the alphabet.

Polyalphabetic cipher

On the other hand, a polyalphabetic cipher adds complexity by using multiple substitutions for the same letter based on a secret key. The Vigenère cipher is a common example, where each letter in the key corresponds to a different shift in the alphabet. This dynamic substitution makes it more challenging for cryptanalysts to decipher the message, providing increased security compared to monoalphabetic ciphers. Poly means

many, and in this case, it means many ways of encrypting each letter, adding an extra layer of protection to the coded message.

In this cipher, a keyword is used to determine different shift values for each letter in the plaintext.

For example:

- **Original:** HELLO
- **Key:** KEY
- **Encrypted:** RIJVS

Here, the first letter *H* is shifted by 10 positions (K in the alphabet), the second letter *E* by 4 positions (I in the alphabet), and so on.

The various roots of ancient cryptography are as follows:

Egyptians

The ancient Egyptians used a primitive form of steganography, which is the practice of hiding a message within another message or medium. They would carve hieroglyphs on the back of a stone slab, then cover the back with a layer of wax and write a harmless message on top of it, making it hard to detect that there was a hidden message. The method of steganography was also used by the Greeks and Romans, who would shave the head of a messenger and tattoo a message on his scalp, this reference is portrayed in a Hollywood movie, and then they used to wait for his hair to grow back before sending him on his way.

Greeks

The Greeks devised a slightly different and simpler method of encrypting messages by wounding a piece of tape around a stick. When the tape was unwound, the writing would appear gibberish. The intended recipient would then use a matching stick to decipher the message. On the other hand, romans used the Caesar Shift Cipher technique for encryption. It involved shifting letters by a fixed number, typically three, to create the coded message. To decode the message, the recipient would subsequently move the letters backwards by the identical magnitude. The Caesar Shift Cipher exemplifies a monoalphabetic cipher.

Emergence of distributed system

Likewise, the concept of distributed systems also has a long history. It dates back to the early days of computing when mainframe computers were connected through networks, where a universal flow of data always ends up with a certain particular node or few

among the system. The initial development of distributed systems has been driven by the demand for expandability, dependability and availability. As the scope of internet broadened and more devices and resources were let out to explore the network, it was the best point to make entry for distributed systems, and to play a crucial role in contemporary computing infrastructure. In the early days of software architecture, monolithic systems were prevalent. These systems combined data access codes, business logic, and user-interface code, making it difficult to separate the layers, such as when the DBMS changes, or reuse components in other applications due to lack of modularity. The progression of distributed computing systems has been substantial since their origins. In the beginning, an individual computer could only execute one job at a time, and it was necessary to have multiple machines running concurrently to carry out multiple tasks.

However, this alone was inadequate to establish a fully distributed system, as it necessitated a method of intercommunication between different computers or software running on them. This resulted in the creation of message-based communication, where information is exchanged between computers using messages, as well as other techniques such as file and database sharing. The advent of multitasking operating systems and personal computers marked a new era in distributed systems. The emergence of operating systems such as Windows, Unix, and Linux enabled the execution of multiple tasks on a single machine. This, in turn, facilitated the construction and operation of entire distributed systems within one or a few interconnected computers via messaging. This development led to the emergence of the **service-oriented architecture (SOA)**, wherein distributed systems were constructed by integrating a set of services running on one or multiple computers. The service interfaces were specified using WSDL (for SOAP) or WADL (for REST), and service consumers employed these interfaces for their client-side implementations. Please refer to the following *Figure 1.1*:

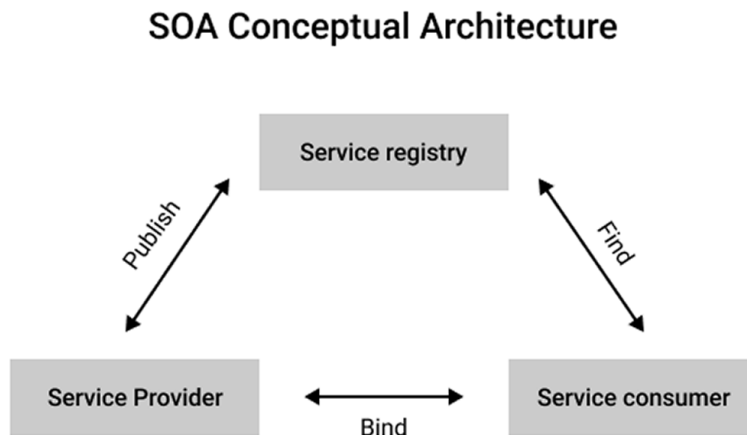


Figure 1.1: Graphical representation of the SOA conceptual architecture.