Blockchain and DLT

A comprehensive guide to getting started with Blockchain and Web3

Nakul Shah

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55519-283

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

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.

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

Monoalphabetic cipher 3

Polyalphabetic cipher 3

Egyptians..4

Greeks 4

Emergence of distributed system 4

Edge computing 6

Cryptography's basic concepts and terminologies 8

Know about cryptography...9

Encryption: A way to secure system..10

Industrial impact of cryptography 12

Evolution of cryptography 12

Public key cryptography 13

RSA algorithm 13

Elliptic curve cryptography 14

Key generation..14

Digital signatures..14

Implementation note...15

Encryption...15

Secure communication 16

Principles of cryptography 17

Encryption algorithms..18

Symmetric-key encryption 18

Data encryption standard 18

Advanced encryption standard 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

Public and private key system......52
Bitcoin network: Proof of work......52
Ethereum network: Proof of stake......52
Applications of blockchain technology......53
Smart contracts......54
Different models of smart legal contracts......54
External......54
Internal......55
Distributed ledger technology......55
Impact of cryptography blockchain......56
Understanding blockchain cryptography......56
Network security......57
Intrusion detection and prevention system......58
Types of intrusion detection and prevention systems (IDPS)......60
Security protocols......60
Security standards......61
Conclusion......64
Question and answers......65
Multiple choice questions......65
Answers......66

2. Introduction to Blockchain Technology......67
Introduction......67
Structure......68
Objectives......68
Rise of blockchain technology......68
Defining blockchain......69
Problems with a centralized system......70
Centralized vs. decentralized vs. distributed architecture......71
Blockchain: A comprehensive network architecture......74
Simplified architecture of blockchain......77
Key characteristics of blockchain architecture......78
Technical definition of a blockchain......80

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

3. Bitcoin.....113
Introduction.....113

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

Bitcoin HD wallet 146
Creating an HD wallet from the seed 148
Derive private child key 148
Derive public child key 149
Transaction script 150
Script address 152
Bitcoin mining 154
History of Bitcoin mining 155
Working of bitcoin mining 155
Structure of a block 159
Block header 160
Genesis block 162
Linking of blocks 163
Type of full nodes 165
Bitcoin core application programming interface 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
Full node 173
Exchange network 174
Nodes communication 175
Simplified payment verification 175
SPV nodes and privacy 176
Transaction pool 176
Blockchain fork 177
Bitcoin testnet 178
Basics of Bitcoin forensic 178
Clustering of address 179
Conclusion 180

Questions and answers 180
Multiple choice questions 181
Answers *182*

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

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

Truffle: Smart contract development....235
Significance of Truffle in smart contract development....236
Remix and test networks....238
Remix: An accessible IDE....238
Importing from GitHub....239
Plugin management....239
Deployment on testnets....239
Additional features....240
Test networks: Simulating blockchains....240
Conclusion....241
Questions and answers....241
Multiple choice questions....242
Answer....243

5. Permissioned Blockchain: Hyperledger Fabric....245
Introduction....245
Structure....246
Objectives....246
Defining permissioned blockchains....247
Architecture of permissioned blockchains....247
Use cases and applications....248
Architecture of Hyperledger Fabric....249
The modular design....249
Why Hyperledger Fabric....250
Chaincode....252
Lifecycle of a chaincode....253
Transaction processing....254
Upgrading....254
Maintenance....255
Scaling....255
The ordering services....255
Membership services....255
Real-world deployments....256

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

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

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

6. Crypto Assets and Cryptocurrencies 295
Introduction 295
Structure 296
Objectives 296

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

Questions and answers 311
Multiple choice questions 312
Answers *313*

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

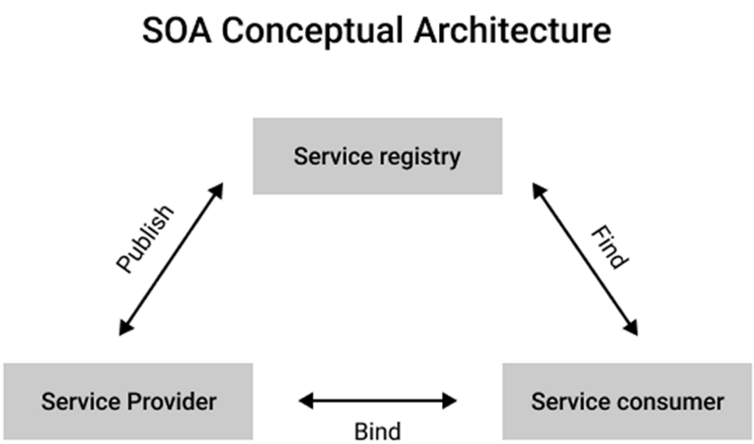

***Figure 1.1**: Graphical representation of the SOA conceptual architecture.*