

Beginning with Web3

*An essential guide to building
dApps in the new internet era*

Ken Huang



www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

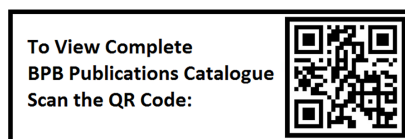
ISBN: 978-93-55517-401

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

My beloved wife:

Queenie

and

*My daughter **Grace** and my son **Jerry***

About the Author



Ken Huang is the author and chief editor of 8 books on Generative Artificial Intelligence and Web3, published respectively by international publishers including Springer, Cambridge University Press, John Wiley, and China Machine Press. He currently serves as the CEO of the AI and Web3 consulting and education company DistributedApps. AI, based in the United States. Additionally, he holds multiple roles including the expert member of the Blockchain Committee of the Chinese Institute of Electronics, the Co-Chair of AI Organization Responsibility Working Group at Cloud Security Alliance and Chair of the Blockchain Security Working Group at the Cloud Security Alliance, GCR. He is also a core contributor to the Generative AI Working Group at the NIST and a core author of the OWASP Top 10 for LLM Applications.

Ken Huang has been invited to provide speaking and consulting services at institutions including the University of California, Berkeley, Stanford University, Peking University, Tsinghua University, Shanghai Jiao Tong University, China Pacific Insurance, and the World Bank in the past.

Moreover, he has given keynote speeches at international conferences, such as:

- The Davos World Economic Forum 2020 Blockchain Conference
- Consensus 2018 in New York
- The American ACM AI & Blockchain Decentralized Annual Conference 2019
- IEEE Technology and Engineering Management Society Annual Meeting 2019
- Silicon Valley World Digital Currency Forum
- Sino-US Blockchain Summit in Silicon Valley

He has also been awarded the "Blockchain 60" Figure Award by the National University Artificial Intelligence and Big Data Innovation Alliance Blockchain Special Committee in China in 2021.

About the Reviewers

- ❖ **Mantas Miklaševičius** is a developer with professional experience in Web3 and backend development. He has designed, implemented, optimized and tested numerous Smart Contracts, primarily for EVM chains.

His main focus is DeFi, as he believes building inclusive decentralized financial services to be both challenging and rewarding

Mantas is currently a Smart Contract Developer for the LendeXe Finance protocol.

- ❖ **Omolaja Oladunjoye** is a dedicated Web3 practitioner with extensive professional experience in the domain of blockchain technology, including blockchain cost optimization, blockchain assessment, blockchain governance, application fitment for blockchain, blockchain operating model, blockchain vendor evaluation, blockchain policy, and blockchain economics. He is a holder of multiple industry certifications in Python, networking, IT support specialist, and blockchain technology.

Oladunjoye specializes in blockchain economics, and enjoys collaborating with clients to maximize their blockchain investments.

Acknowledgement

My heartfelt thanks are extended to my family and friends for their constant support and encouragement throughout the process of writing this book. Special mention goes to my wife, Queenie, and my children, Grace and Jerry, for their understanding and love.

The journey to the completion of this book was significantly enhanced by the guidance and expertise provided by BPB Publications. Their support was crucial in navigating the complexities of publishing. The process involved numerous revisions, benefiting from the collaborative efforts of reviewers, technical experts, and editors, whose contributions have been instrumental in refining this work.

Additionally, I am profoundly grateful for the pioneers of the Web3 community, whose efforts in building a self-sovereign and decentralized internet have paved the way for the subjects discussed in this book. Their pioneering work has laid the foundation for a new digital era based on value.

Lastly, my appreciation extends to all the readers who have shown interest in this book. Your support and encouragement have played a pivotal role in making this project a reality. Thank you for believing in the importance of this work and for your invaluable support.

Preface

Beginning with Web3 is your comprehensive guide to navigating the complex yet captivating world of Web3 and blockchain technology. This book is designed to provide you with a deep understanding of the decentralized web, equipping you with the knowledge and skills necessary to develop **decentralized applications (dApps)**. From the foundational principles of Web3 and the Ethereum blockchain to the intricacies of security, storage, and development tools, this guide is a gateway to the future of the internet. As you embark on this journey, you will discover the challenges and opportunities of Web3 development, inspiring you to contribute to the growth and innovation of this exciting domain. Let us explore the new era of the internet together and build the future, one dApp at a time.

This book has three distinct sections, each dedicated to a different aspect of Web3 development. This organization helps readers systematically grasp the breadth and depth of Web3, from foundational concepts to the development of decentralized applications and beyond. Below is an overview of each section and its chapters:

Section I: Foundations of Web3 and Blockchain

This section lays the groundwork for understanding Web3 and blockchain technology, providing essential knowledge needed to navigate the decentralized web.

Chapter 1: Introduction to Web3 - This chapter offers a primer on the decentralized internet, outlining the shift from traditional web paradigms to the Web3 philosophy.

Chapter 2: Understanding the Ethereum Blockchain - This chapter focuses on Ethereum, introducing its key components and importance in dApp development.

Chapter 3: Web3 Node Infrastructure - The chapter explains the role and types of nodes in maintaining a decentralized network.

Chapter 4: Wallets and Key Management in Web3 - This chapter covers the critical aspects of securing digital assets through effective wallet and key management techniques.

Section II: Security and Storage in Web3

This section discusses the security challenges and storage solutions in the Web3 ecosystem, emphasizing how to protect dApps and utilize decentralized storage.

Chapter 5: Security in Web3 Development - This chapter highlights the importance of security, detailing common threats and mitigation strategies.

Chapter 6: Introduction to Decentralized Storage - This chapter introduces decentralized storage, explaining its benefits and operational mechanisms.

Section III: How to Develop Web3 Applications

Guides readers through the practical aspects of Web3 application development, from utilizing development tools to creating specific types of dApps.

Chapter 7: Tools for Web3 Development - The chapter provides an overview of essential development tools and their applications in building dApps.

Chapter 8: DeFi and NFT dApp Development - This chapter discusses the development of DeFi and NFT applications, two of the most prominent use cases in Web3.

Chapter 9: Building dApps on Popular Chains and Protocols - This chapter explores dApp development across various blockchain platforms beyond Ethereum.

Chapter 10: ChatGPT and Web3 Development - This chapter looks at the integration of AI, specifically Generative AI application such as ChatGPT, into dApp development, highlighting new possibilities.

Each section of **Beginning with Web3** is carefully designed to progress readers from foundational knowledge to practical application, ensuring a comprehensive understanding of how to build, secure, and innovate within the Web3 space.

Beginning with Web3 simplifies the complexities of Web3 development, providing a clear path from foundational concepts to advanced application building. By the end of this book, you will be well-equipped to contribute to the revolutionary world of Web3. Let us embark on this journey to build the future of the internet, together.

Code Bundle and Coloured Images

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

<https://rebrand.ly/2tpx25p>

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

<https://github.com/bpbpublications/Beginning-with-Web3>

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

Section I: Foundations of Web3 and Blockchain.....	1
1. Introduction to Web3.....	3
Introduction.....	3
Structure.....	3
Objectives	4
Evolution from Web1 to Web3.....	4
<i>Birth and growth of Web1</i>	<i>4</i>
<i>Transition to Web2</i>	<i>5</i>
<i>Emergence of Web3</i>	<i>6</i>
Fundamental principles of Web3	8
<i>Decentralization</i>	<i>8</i>
<i>Privacy and user control</i>	<i>10</i>
<i>Trustless systems</i>	<i>11</i>
Comparing Web2 and Web3	12
<i>Understanding Web2</i>	<i>13</i>
<i>Key features of Web3</i>	<i>14</i>
<i>Transition from Web2 to Web3</i>	<i>15</i>
Role of blockchain in Web3.....	16
<i>Understanding blockchain</i>	<i>17</i>
<i>Blockchain as a foundation of Web3.....</i>	<i>18</i>
<i>Technical challenges of blockchain technology in Web3.....</i>	<i>19</i>
Understanding smart contracts and peer-to-peer networks.....	22
<i>Introduction to smart contracts</i>	<i>22</i>
<i>Peer-to-peer networks and decentralization.....</i>	<i>23</i>
<i>Interaction of smart contracts and peer-to-peer networks in Web3.....</i>	<i>24</i>
<i>Conclusion.....</i>	<i>25</i>
Questions	26
Keywords.....	27

2. Understanding the Ethereum Blockchain	29
Introduction.....	29
Structure.....	30
Objectives	30
Overview of Ethereum blockchain	30
<i>History of Ethereum</i>	31
Key Ethereum architecture concepts.....	32
<i>Ethereum nodes</i>	33
<i>Full nodes</i>	33
<i>Light nodes</i>	33
Accounts.....	34
Transactions	35
Blocks.....	37
Gas.....	37
<i>EIP and EIP-1559 impact on GAS</i>	38
Ether	39
<i>Ether as a means of exchange</i>	40
<i>Ether as incentive and fuel</i>	40
<i>Ether denominations and creation</i>	42
<i>Ether's role in the ecosystem</i>	42
Consensus algorithm.....	42
<i>Proof-of-work and Ethash</i>	43
<i>The Merge: Transition to proof-of-stake</i>	43
Smart contracts	44
<i>Defining smart contracts</i>	45
<i>Ethereum and smart contracts</i>	45
<i>The language of smart contracts: Solidity</i>	45
<i>Smart contracts use cases</i>	46
<i>The future of smart contracts</i>	47
Ethereum virtual machine.....	48
<i>The Ethereum ecosystem and EVM's position</i>	48
<i>The architecture of the Ethereum virtual machine</i>	49

Decentralized applications.....	50
<i>Tokens</i>	51
<i>Oracles</i>	52
Scalability of Ethereum blockchain.....	53
<i>Layer 2 scaling</i>	53
<i>Sharding</i>	55
Governance and development	55
Interacting with Ethereum network.....	57
<i>Prerequisites</i>	57
<i>Understanding libraries</i>	58
<i>Ethers.js</i>	58
<i>Key features of Ethers.js</i>	58
<i>Web3.js</i>	58
<i>Distinctions between Ethers.js and Web3.js</i>	59
<i>Comparisons with examples</i>	59
Conclusion.....	60
Points to remember	60
Questions	61
Keywords.....	62
3. Web3 Node Infrastructure	63
Introduction.....	63
Structure.....	63
Objectives	64
Types of nodes in a blockchain network.....	64
<i>Full nodes</i>	64
<i>The essential nature of full nodes in blockchain</i>	64
<i>Full nodes: The guardians of network security and decentralization</i>	65
<i>Demands of running a full node: Hardware prerequisites</i>	66
<i>Light nodes</i>	66
<i>Understanding light nodes in the blockchain ecosystem</i>	67
<i>Use cases and advantages of light nodes</i>	67
<i>Working of SPV nodes</i>	67

Merkle tree	68
Using a Merkle tree in an SPV client.....	68
Inherent limitations of light nodes.....	69
Archive nodes	70
Archive nodes and their distinctive features.....	70
Use cases: Debugging and deep blockchain analysis	70
Operational challenges and considerations.....	71
Setting up an Ethereum node with Geth	71
Local PoS Node Setup	71
Prerequisites.....	71
Get the binaries	72
Clone and build Prysm	72
Configuration files.....	72
Generate genesis state	73
Start execution and consensus clients	73
Adding peer nodes.....	73
Summary.....	74
Interacting with your node	74
Introduction to node interaction.....	74
Geth's JavaScript console: The direct gateway	74
Geth's RPC interface: The programmable gateway.....	75
web3.js: Bridging dApps and nodes.....	75
Additional tools and extensions.....	76
Understanding node synchronization.....	76
Different synchronization modes	76
Essence of blockchain synchronization	76
Full nodes synchronization.....	76
Archive nodes synchronization.....	78
Light nodes synchronization.....	78
Consensus layer syncing.....	78
Role of synchronization in network consistency.....	78
Network consistency: A cornerstone of blockchain technology	78

<i>Synchronization: The path to network consistency</i>	79
<i>Full synchronization: Upholding network integrity</i>	79
<i>Light synchronization: Consistency for constrained devices</i>	79
<i>Network consistency beyond synchronization</i>	79
<i>Benefits of network consistency</i>	80
<i>Troubleshooting synchronization issues</i>	80
<i>Understanding the nature of synchronization issues</i>	80
<i>Network connectivity issues</i>	80
<i>Disk space and I/O Issues</i>	80
<i>Software bugs or corruptions</i>	81
<i>Node configuration issues</i>	81
<i>Time sync issues</i>	81
<i>General best practices</i>	82
Role of nodes in network security	82
<i>Transaction validation</i>	82
<i>Breaking down a transaction</i>	82
<i>Step-by-step transaction validation by nodes</i>	83
<i>The collective role of nodes in transaction validation</i>	83
<i>Beyond validation: Nodes as gatekeepers</i>	84
<i>Consensus enforcement</i>	84
<i>The essence of consensus in blockchain</i>	84
<i>Nodes: The enforcers of consensus</i>	84
<i>Consensus mechanisms and their impact on security</i>	86
<i>Consensus enforcement, blockchain immutability and finality</i>	86
<i>Network resilience</i>	87
<i>Decentralization: The heart of resilience</i>	87
<i>Nodes: The pillars of a resilient network</i>	87
<i>Case study: The bitcoin network</i>	88
<i>Decentralization versus centralization</i>	88
<i>Enhancing resilience</i>	88
Use RPC nodes for your dApp development	89
<i>Understanding RPC nodes</i>	89

<i>RPC nodes: The bridge to the blockchain</i>	89
<i>Working of RPC nodes</i>	89
<i>Why use RPC nodes in dApp development?</i>	90
<i>Choosing a reliable RPC service</i>	91
<i>Setting up an RPC node</i>	91
<i>Why set up your own RPC node?</i>	91
<i>Integrating RPC nodes in dApps</i>	93
<i>Connecting to the RPC node</i>	93
Conclusion.....	95
Questions.....	96
Keywords.....	97
4. Wallets and Key Management in Web3	99
Introduction.....	99
Structure.....	100
Objectives	100
Understanding cryptographic keys.....	100
<i>Public and private keys</i>	100
<i>Generating key pairs</i>	101
<i>Mathematical relationship</i>	101
<i>Role in securing transactions</i>	102
<i>Key takeaways</i>	102
<i>Digital signatures</i>	102
<i>Generating digital signatures</i>	103
<i>Verifying digital signatures</i>	104
<i>Importance in blockchain transactions</i>	104
<i>Key takeaways</i>	104
<i>Role of cryptographic keys in blockchain</i>	104
<i>Transaction validation</i>	105
<i>Data security</i>	105
<i>Smart contracts and dApps</i>	105
<i>Address generation</i>	105
<i>Establishing trust in a trustless environment</i>	105

<i>Key takeaways</i>	105
Overview of wallet types in Web3	106
<i>Software wallets</i>	106
<i>Types of software wallets</i>	106
<i>Pros and cons of software wallets</i>	107
<i>Safety measures with software wallets</i>	107
<i>Hardware wallets</i>	108
<i>Advantages of hardware wallets</i>	108
<i>Common models in the market</i>	108
<i>Using a hardware wallet</i>	109
<i>Key takeaways</i>	109
<i>Account abstraction: A new era for Ethereum wallets</i>	109
<i>The essence of account abstraction</i>	110
<i>Account abstraction details</i>	110
<i>Comparison of wallet types</i>	112
Key generation with Ethereum	114
<i>Setting up Ethereum</i>	114
<i>Prerequisites</i>	114
<i>Installation process</i>	114
<i>Initial configuration</i>	115
<i>Generating keys with Ethereum</i>	115
<i>Step 1: Initialize Ethereum</i>	116
<i>Step 2: Generate a new key pair</i>	116
<i>Step 3: Understanding the implications</i>	116
<i>Step 4: Backup and safe storage</i>	117
<i>Creating wallets with Ethereum</i>	117
<i>Step 1: Initialize Ethereum</i>	117
<i>Step 2: Create a new Wallet instance</i>	117
<i>Step 3: Access the wallet's address</i>	117
<i>Step 4: Sign transactions</i>	118
<i>Step 5: Import and export wallets</i>	118
Best practices for wallet security	118

Using encryption.....	119
Understanding encryption.....	119
Why encryption matters for private keys.....	119
Steps to encrypt your private key	119
Decryption	120
Backing up your wallet	121
Importance of regular backups	121
How to back up your wallet	121
Secure usage habits.....	122
Regular software updates.....	122
Use of secure networks.....	123
Multi-factor authentication	123
Beware of phishing attempts	123
Use trusted third-party services	123
Regularly monitor your wallet.....	123
Limit exposure with cold and hot wallets	124
Educate yourself.....	124
Key management and recovery.....	124
Dealing with key loss	124
The gravity of losing a private key.....	124
Why traditional recovery does not apply	125
Steps to take after key loss.....	125
Key recovery methods.....	127
Mnemonic seed phrases.....	127
Keystore files	127
Physical paper wallets.....	128
Hardware wallet recovery	128
Importance of seed phrases	128
Seed phrase.....	128
Working of a seed phrase.....	129
Seed phrase, private key and address.....	129
Relationship and security implications.....	130

Example..... 130
Storing seed phrases securely..... 131
 Conclusion..... 131
 Questions..... 132
 Keywords..... 133

Section II: Security and Storage in Web3 135

5. Security in Web3 Development..... 137
 Introduction..... 137
 Structure..... 138
 Objectives 138
 Common vulnerabilities in Web3..... 138
 Top smart contract vulnerability..... 139
 Reentrancy attacks 139
 Oracle manipulation 141
 Gas griefing..... 143
 Transaction order dependence attacks..... 144
 Force feeding attacks 145
 Timestamp dependence..... 146
 Denial of service 147
 Information and function exposure..... 149
 Bridge attacks 150
 Security of consensus model in blockchain 151
 Incorrect input validation in cross chain protocol 151
 Lack of cross contract access control in blockchain bridges 151
 Rug pull..... 152
 Miner extractable value..... 153
 Uncle bandit attacks..... 153
 Time Bandit attacks..... 154
 Mitigating security risks in Web3 development 155
 Best coding practices 155
 Latest Solidity versions 155

<i>Proper error handling</i>	156
<i>Conservative estimates for gas limits</i>	156
<i>Code audits and testing</i>	156
<i>Use of modular contracts</i>	156
<i>Why modular contracts?</i>	157
<i>Implementing modular contracts</i>	157
<i>Security considerations</i>	157
<i>Regular code reviews</i>	158
<i>Importance of regular code reviews</i>	158
<i>Effective code review practices</i>	158
<i>Automated contract security analysis with MythX and Slither</i>	159
<i>Introduction to MythX</i>	159
<i>MythX: An overview</i>	159
<i>Integrating MythX into the development process</i>	159
<i>Benefits of using MythX</i>	160
<i>Introduction to Slither</i>	161
<i>Using Slither: A tutorial</i>	161
<i>Advantages of static analysis with Slither</i>	162
<i>Other smart contract security auditing tools</i>	162
<i>Oyente</i>	162
<i>Securify</i>	163
<i>SmartCheck</i>	163
<i>Echidna</i>	163
<i>Manticore</i>	163
<i>Importance of auditing and testing in Web3</i>	163
<i>Testing smart contracts</i>	164
<i>Security auditing</i>	165
<i>Role of testnets</i>	166
<i>Security considerations in decentralized storage</i>	167
<i>Overview of decentralized storage platforms</i>	167
<i>Data encryption and privacy</i>	168
<i>Access control in decentralized storage</i>	169

Conclusion.....	170
Questions.....	171
Keywords.....	172
6. Introduction to Decentralized Storage.....	175
Introduction.....	175
Structure.....	175
Objectives	176
Introduction to IPFS.....	176
<i>Principles of IPFS.....</i>	<i>176</i>
<i>Decentralization.....</i>	<i>177</i>
<i>Content addressing</i>	<i>177</i>
<i>Peer-to-peer networking.....</i>	<i>177</i>
<i>The confluence of principles</i>	<i>177</i>
IPFS architecture.....	178
Objects.....	178
Files	178
Naming	178
Routing	178
Unifying the components.....	178
Content-addressed data storage.....	179
Understanding content-addressed storage.....	179
Benefits of content addressing.....	179
Content addressing and IPFS	179
Setting up and interacting with IPFS.....	180
<i>Installing an IPFS node</i>	<i>180</i>
Prerequisites.....	180
Downloading and installing IPFS.....	180
Initializing the IPFS node.....	181
Starting the IPFS node.....	181
Adding files to the network	181
Preparing your data	181
Adding the file to IPFS.....	182

<i>Broadcasting the file to the network</i>	182
<i>Retrieving data with content identifiers</i>	182
<i>Understanding content identifiers</i>	182
<i>Retrieving a file</i>	183
<i>Storing and retrieving data in a decentralized way</i>	183
<i>Protocols for data distribution</i>	183
<i>Role of peers</i>	183
<i>BitSwap protocol</i>	184
<i>Distributed hash table</i>	184
<i>Ensuring efficient data distribution</i>	184
<i>Role of content identifiers in retrieval</i>	184
<i>Content identifiers and content-addressed storage</i>	185
<i>Data retrieval with content identifiers</i>	185
<i>Advantages of content identifiers in retrieval</i>	185
<i>Achieving redundancy in a decentralized network</i>	185
<i>Importance of redundancy</i>	186
<i>Data replication in IPFS</i>	186
<i>Pinning for persistent storage</i>	186
<i>Achieving redundancy through replication and pinning</i>	186
<i>Understanding Filecoin</i>	186
<i>Introduction to the Filecoin protocol</i>	187
<i>Storage miners</i>	187
<i>Deals</i>	187
<i>Proofs of storage</i>	187
<i>Incentivizing decentralized storage</i>	188
<i>Role of FIL tokens</i>	188
<i>Economics of decentralized storage</i>	189
<i>Balancing supply and demand</i>	189
<i>Relationship between Filecoin and IPFS</i>	189
<i>Complementary roles</i>	189
<i>IPFS and Filecoin integration</i>	190
<i>Joint contribution to the decentralized web</i>	190

Ensuring data availability and privacy	190
<i>Data replication techniques</i>	190
<i>Understanding data replication</i>	190
<i>Replication in IPFS</i>	191
<i>Replication in Filecoin</i>	191
<i>Redundancy and data availability</i>	191
<i>Data privacy and encryption</i>	191
<i>Need for data privacy</i>	191
<i>Role of encryption</i>	192
<i>Client-side encryption</i>	192
<i>Encryption and decentralized storage</i>	192
<i>Verifying data integrity and availability</i>	192
<i>Ensuring data integrity with cryptographic hashes</i>	192
<i>Proofs of replication and retrieval</i>	192
<i>Verifying data integrity and availability</i>	193
Storing files in Filecoin local node	193
Arweave	196
<i>Core concepts of Arweave</i>	196
<i>Integration in Web3 development</i>	196
<i>Implementing Arweave in a sample dApp</i>	197
Conclusion	197
Questions	198
Keywords	199

Section III: How to Develop Web3 Applications..... 201

7. Tools for Web3 Development.....	203
Introduction.....	203
Structure.....	204
Objectives	204
Understanding the role of Truffle and Hardhat.....	204
<i>Introduction to Truffle</i>	205
<i>Installation of Truffle</i>	205

Core functionalities of Truffle.....	205
Role of Truffle in smart contract development	205
Unveiling Hardhat	206
Unique features of Hardhat.....	206
Installation and usage of Hardhat.....	206
Role of Hardhat in Ethereum development	209
Other Web3 development platforms.....	209
Compiling and deploying smart contracts	210
Writing smart contracts.....	211
Writing smart contracts.....	211
Compiling smart contracts.....	211
Deploying smart contracts	212
Using Ganache for local blockchain development	213
Setting up Ganache	213
Installation	213
Creating a workspace	213
Understanding the interface	214
Simulating transactions with Ganache.....	214
Executing transactions	215
Interpreting transaction details	216
Using Ganache with Truffle and Hardhat.....	216
Configuring Truffle with Ganache	216
Configuring Hardhat with Ganache	217
Setting up and using Infura	217
Infura and its uses.....	218
Setting up Infura.....	218
Integrating Infura with dApps.....	219
Prerequisites	220
Integrating Infura with Web3.js.....	220
Integrating Infura with ethers.js.....	220
Best practices for Web3 development.....	221
Smart contract security.....	221

Efficient gas usage	222
Simplifying code logic	223
Optimizing data storage	223
Using appropriate function visibility	224
Building user friendly dApps.....	224
Clear and intuitive interface	224
Graceful handling of transactions and errors	225
Making dApps accessible to non-technical users.....	225
Use Chainlink to get randomness for your dApps	225
Prerequisites of using Chainlink VRF	225
Understanding Chainlink VRF	225
Working of Chainlink VRF	226
Methods of requesting randomness.....	226
Creating a custom lottery contract with Chainlink VRF	226
Use Ethereum Name Service.....	228
Using ENS in Truffle.....	229
Conclusion.....	230
Questions.....	230
Keywords.....	231
8. DeFi and NFT dApp Development	233
Introduction.....	233
Structure.....	233
Objectives	234
Understanding DeFi and key protocols	234
Basics of DeFi.....	234
Principles of DeFi.....	234
Value proposition of DeFi	235
Risks of DeFi	235
Democratizing access to financial services	236
Sample DeFi protocols: Aave and Uniswap.....	236
Aave.....	236
Uniswap.....	239

<i>Liquidity pools and yield farming</i>	241
<i>Liquidity pools</i>	241
<i>Yield farming</i>	242
Developing a DeFi dApp	244
<i>Defining the smart contract</i>	244
<i>Deploy smart contract</i>	248
<i>Test smart contract</i>	250
<i>Mocha</i>	254
<i>Chai</i>	254
<i>UI or front end</i>	257
<i>React for web applications</i>	257
<i>React Native for mobile applications</i>	257
<i>Common features in DeFi UI</i>	258
<i>Development approach</i>	258
Introduction to Non Fungible Tokens	259
<i>Basics of NFTs</i>	259
<i>Unique properties of NFTs</i>	259
<i>Why does uniqueness matter</i>	259
<i>History of NFTs</i>	260
<i>Emergence of NFT as a pervasive topic of interest</i>	260
<i>Impact of NFTs</i>	261
Creating your own NFT with ERC 721 and ERC 1155.....	261
<i>Understanding ERC 721</i>	261
<i>Famous use cases of ERC 721</i>	262
<i>Exploring ERC 1155</i>	262
<i>Famous use cases of ERC 1155</i>	264
<i>Creating your own NFT</i>	264
Practical applications of DeFi and NFTs	266
<i>DeFi in the real world</i>	266
<i>Lending and borrowing</i>	266
<i>Stablecoins</i>	266
<i>Decentralized exchanges</i>	267

Yield farming and liquidity mining	267
Insurance.....	267
Asset management	267
NFTs beyond digital art.....	268
Gaming.....	268
Real estate.....	268
Intellectual property.....	268
Collectibles and memorabilia.....	269
Domain names	269
Future trends in DeFi and NFTs.....	269
Real-world asset tokenization	269
Interoperability.....	269
Regulation.....	269
Layer 2 solutions and scalability.....	270
Fractional ownership.....	270
NFTs in virtual reality.....	270
Conclusion.....	270
Questions.....	270
Keywords.....	271
References.....	272
9. Building dApps on Popular Chains and Protocols	273
Introduction.....	273
Structure.....	273
Objectives	274
Understanding Ethereum alternatives.....	274
Polkadot.....	274
Polkadot's architecture.....	274
Relay Chain.....	274
Parachains.....	275
Bridges.....	275
High scalability	276
Interoperability.....	276

<i>Binance Smart Chain</i>	276
<i>BNB Chain's architecture</i>	276
<i>Interacting with BNB Chain</i>	277
<i>Ethereum alternatives comparison</i>	277
<i>Solana</i>	278
<i>Polygon</i>	278
<i>Polkadot</i>	279
<i>NEAR</i>	279
<i>Cosmos</i>	280
<i>Algorand</i>	282
<i>Aptos</i>	283
<i>Sui</i>	283
<i>Deploying smart contracts on different chains</i>	285
<i>Developing for Polkadot</i>	285
<i>Understanding Polkadot and Substrate</i>	286
<i>Working with Polkadot</i>	286
<i>Writing a Substrate contract</i>	288
<i>Compiling and deploying the contract</i>	289
<i>Interacting with the contract</i>	290
<i>Understanding Gas in Polkadot</i>	291
<i>Developing for BNB Chain</i>	292
<i>Setting up the development environment</i>	292
<i>Writing a smart contract</i>	292
<i>Compiling and deploying the contract</i>	293
<i>Interacting with the contract</i>	293
<i>Exploring Layer 2 solutions</i>	294
<i>Optimistic rollups: Scalability and affordability</i>	294
<i>Understanding optimistic rollups</i>	294
<i>Achieving scalability and affordability</i>	294
<i>Deploying and interacting with dApps on optimistic rollups</i>	295
<i>ZK Rollups: Enhanced privacy and performance</i>	295
<i>Understanding ZK Rollups</i>	296

<i>Ensuring privacy and transaction speed</i>	296
<i>Deploying and interacting with dApps on ZK Rollups</i>	296
Understanding multi-chain deployment	298
<i>Case for multi-chain deployment</i>	298
<i>Access to different user bases</i>	298
<i>Avoidance of single platform dependency</i>	298
<i>Enhanced resilience and security</i>	299
<i>Capitalizing on unique features</i>	299
<i>Challenges in multi-chain deployment</i>	299
<i>Cross-chain communication</i>	299
<i>Inconsistency in smart contract languages and standards</i>	300
<i>Multiple wallets and user experience</i>	300
<i>Varying gas fees and transaction times</i>	300
<i>Governance and regulatory challenges</i>	301
<i>Strategies for multi-chain deployment</i>	301
<i>Choosing the right chains</i>	301
<i>User interface and experience considerations</i>	301
<i>Managing updates across chains</i>	302
<i>Governance and community engagement</i>	302
Importance of blockchain interoperability	302
<i>Blockchain interoperability</i>	302
<i>Need for interoperability</i>	302
<i>Working of blockchain interoperability</i>	303
<i>Mechanisms enabling interoperability</i>	303
<i>Benefits of interoperability</i>	304
<i>Wider adoption of blockchain technology</i>	304
<i>Efficient cross-chain transactions</i>	304
<i>Diverse and resilient dApp ecosystems</i>	304
<i>Facilitating innovation and collaboration</i>	305
<i>Enhancing liquidity and market efficiency</i>	305
<i>Future of interoperability</i>	305
Conclusion	306

Questions.....	306
Keywords.....	308
10. ChatGPT and Web3 Development.....	311
Introduction.....	311
Structure.....	312
Objectives	312
Introduction to OpenAI's ChatGPT	313
<i>Understanding ChatGPT</i>	313
<i>ChatGPT API</i>	314
<i>ChatGPT safety measures</i>	315
Potential use cases of ChatGPT in Web3.....	316
<i>ChatGPT and NFTs</i>	316
<i>ChatGPT in decentralized finance</i>	318
<i>User experience enhancement</i>	319
Integrating ChatGPT into a Web3 dApp.....	320
<i>Setting up ChatGPT API</i>	320
<i>Integrating ChatGPT into dApp</i>	322
<i>Customizing the API request to ChatGPT</i>	323
Benefits of AI and blockchain integration.....	324
<i>Enhanced security</i>	324
<i>Optimized decision-making</i>	326
<i>Improved scalability</i>	327
Future directions: AI in the decentralized web.....	328
<i>Ongoing developments</i>	328
<i>Challenges and opportunities</i>	330
<i>Future of AI in Web3</i>	331
Conclusion.....	332
Questions.....	333
Keywords.....	334
Index	337-347

Section - I

Foundations of

Web3 and Blockchain

This section lays the groundwork for understanding Web3 and blockchain technology, providing essential knowledge needed to navigate the decentralized web.

CHAPTER 1

Introduction to Web3

Introduction

This chapter provides a comprehensive introduction to Web3, the next evolution of the internet. We will trace the progression from the early read-only internet (Web1) to the social, participatory platforms of Web2, and finally to the emerging decentralized and user-controlled vision of Web3.

The fundamental principles and technologies driving this paradigm shift are explored in the chapter, including decentralization, blockchain, smart contracts, and peer-to-peer networks. We will compare the Web2 and Web3 models, analyzing how Web3 addresses the centralization of power and lack of user control that characterize today's internet landscape.

While Web3 promises a more open, decentralized, and user-centric web, we will also critically examine the challenges and tradeoffs involved in this transition. As we stand at the cusp of this new internet era, this chapter aims to provide a solid foundation for understanding the possibilities and complexities of Web3.

Structure

The chapter will cover the following topics:

- Evolution from Web1 to Web3

- Fundamental principles of Web3
- Comparing Web2 and Web3
- Role of blockchain in Web3
- Understanding smart contracts and peer-to-peer networks

Objectives

By the end of this chapter, readers will be able to comprehend the evolution of the internet from its origins as Web1 to the social, participatory platforms of Web2, and now the emerging paradigm of Web3. They will be able to understand the fundamental principles underpinning Web3 including decentralization, user control, privacy, and trustless systems.

Readers will be able to recognize core Web3 technologies like blockchain, smart contracts, and peer-to-peer networks and how they enable a decentralized web. They will be able to appreciate how Web3 differs from Web2, particularly regarding centralization of power and user control over data. Readers will gain insight into the role of blockchain as the foundational infrastructure for Web3 and the associated technical challenges. They will also understand how technologies like smart contracts and peer-to-peer networks interact to enable decentralized applications.

After going through this chapter, the reader will be able to identify key opportunities and challenges involved in the transition from Web2 to Web3, and be equipped with the foundational knowledge to explore the technologies and implications of Web3 further.

Evolution from Web1 to Web3

This section traces the development of the Internet from its early stages as Web1, through the interactive platform of Web2, and finally to the decentralized and democratized vision of Web3.

Birth and growth of Web1

This subsection delves into the initial days of Web1, examining its design, functionality, and limitations.

The advent of the **World Wide Web**, or what we now refer to as Web1, was a revolutionary moment in the history of technology and communication. First proposed by *Tim Berners-Lee* in 1989 at CERN, the European research organization, Web1 began as a project to facilitate information sharing among scientists in universities and institutes worldwide.

The initial design of Web1 was quite rudimentary, with web pages consisting of simple text and hyperlinks. These pages were static, meaning they were pre-built and did not

change in response to user interaction. Users could read and navigate the information, but they could not contribute or change the content. Web1 was largely a read-only platform, a digital library where people could find information but had minimal ways to interact with it.

The primary language used to create these web pages was the **Hyper Text Markup Language (HTML)**. HTML allowed web developers to structure text, insert hyperlinks, and later, add images. Despite its simplicity, HTML was a powerful tool for presenting information on the web. It provided the basic structure for web pages and set the foundation for more complex web development tools and languages to come.

The functionality of Web1 was primarily centered around information retrieval. Search engines like AltaVista, Yahoo!, and later Google, were developed to help users find relevant information amidst the rapidly growing volume of web content. The function of these search engines was to crawl the web, indexing pages to make them searchable by keyword. This marked a significant step in making the internet more accessible and useful to the average user.

However, Web1 had its limitations. The lack of interactivity was a major drawback. While users could read and navigate between pages, they could not contribute their own content or interact with other users. Web1 was largely a one-way street, with information flowing from webmasters to users, but not the other way around.

Web1 also lacked the sophisticated design capabilities that we take for granted today. Early web pages were primarily text-based, with few images and virtually no multimedia content. The layout and design options were limited, creating a plain and homogeneous browsing experience. As a result, Web1 was not particularly engaging or immersive, especially compared to what was to come with Web2.

Security was another concern with Web1. As the internet began to grow, so did the risks associated with data privacy and security. However, the security protocols and infrastructure necessary to protect user data were only partially developed during the Web1 era. This led to various security challenges, some of which persist to this day.

Despite these limitations, the birth and growth of Web1 represented a monumental shift in the way information was shared and accessed. It democratized access to information, enabling anyone with an internet connection to access a wealth of knowledge from anywhere in the world. Web1 set the stage for the more interactive, user-centered versions of the web that were to come. As we move further into the era of Web3, it is important to remember and understand the roots of the internet in Web1, as it laid the groundwork for all subsequent developments.

Transition to Web2

The transition from Web1 to Web2 marked a profound shift in the way people interacted with the internet. Where Web1 was a largely static, read-only platform, Web2 evolved into

a dynamic, participatory medium. This transition was not abrupt but rather a gradual shift fueled by advances in technology and changing user expectations.

The dawn of Web2 brought with it the concept of the **participatory web**. Users were no longer mere consumers of information, but they also became creators and contributors. This was made possible by the advent of platforms that allowed user-generated content. Social media platforms like Facebook, Twitter, and Instagram, blogging sites like Blogger and WordPress, and video-sharing platforms like YouTube transformed the internet into a space of active participation.

The rise of social media was a defining aspect of the Web2 era. These platforms provided users with tools to connect, share, and engage with each other in ways previously unimaginable. They gave voice to individuals, allowing them to share their thoughts, experiences, and ideas with a global audience. At the same time, they also created new channels for information flow, altering traditional media landscapes and giving rise to phenomena like viral content and influencer culture.

The emphasis on user participation also had a significant impact on businesses. Traditional business models had to adapt to the new digital landscape. Companies began to recognize the importance of online presence and started to leverage social media platforms for marketing, customer engagement, and brand building. The power of online reviews and ratings became evident as they significantly influenced purchasing decisions.

Web2 also ushered in the era of **web applications**. These were interactive programs that ran within the browser, providing richer and more engaging user experiences. Examples include Gmail, Google Maps, and Facebook. These applications utilized technologies like **Asynchronous JavaScript and XML (AJAX)**, which allowed web pages to update and display new data without the need for a full-page refresh, making the user experience much more dynamic and interactive.

However, this new era had its own challenges. The explosion of user-generated content led to concerns about data privacy and security. As users began sharing more personal information online, the risk of data breaches and misuse of information increased. The shift towards free, ad-supported services also raised questions about data ownership and surveillance.

In conclusion, the transition to Web2 marked a significant evolution in the Internet's history. It moved us from a static, one-way information highway to a dynamic, two-way interaction platform. It democratized content creation, empowered users, and transformed business models. As we look towards the future of the internet in Web3, understanding the journey and impact of Web2 is crucial.

Emergence of Web3

As the internet continues to evolve, we are now witnessing the emergence of Web3. This new iteration of the web represents a significant shift from the interactive, user focused

Web2 to a decentralized and autonomous system. Web3 is envisioned as a truly open and permissionless network, one that extends the user-centricity of Web2 while addressing its limitations.

The primary driver behind the shift to Web3 is the desire for greater decentralization. Web2, for all its advances, still relies heavily on large, centralized entities that control platforms, data, and services. This centralization has raised concerns about data privacy, ownership, and monopolistic control. Web3 aims to address these issues by moving away from centralized control and towards a decentralized network where no single entity has absolute power.

Web3 also seeks to enhance privacy and give users more control over their data. The Web2 model relies heavily on the collection and monetization of user data, often without explicit consent or compensation for users. Web3 proposes a new model where users maintain control of their own data, deciding who can access it and how it can be used. This change aims to restore data ownership to individuals and reduce the power of large corporations.

Another key feature of Web3 is the concept of a trustless system. In a Web3 world, trust is built into the system itself through cryptographic guarantees rather than being dependent on intermediaries. This allows for peer-to-peer interactions and transactions without the need for a trusted third party, reducing the potential for fraud and enhancing security.

Web3 also brings with it the potential for more economic inclusivity. By utilizing blockchain technology and cryptocurrencies, Web3 can facilitate peer-to-peer transactions without the need for traditional financial institutions. This could potentially provide financial services to those who are currently unbanked or underbanked, democratizing access to financial resources.

The rise of Web3 technologies, such as blockchain, smart contracts, and **decentralized applications (dApps)**, are critical to this transformation. Blockchain provides decentralized infrastructure, smart contracts enable autonomous transactions, and dApps provide user interfaces that tie everything together.

However, the transition to Web3 is not without its challenges. Technical complexity, scalability issues, regulatory uncertainty, and public understanding are all hurdles that need to be overcome. Furthermore, while the promise of decentralization is appealing, it also raises new questions about governance, accountability, and security that are yet to be fully addressed.

The shift from Web2 to Web3 is driven by the pursuit of greater decentralization, enhanced user privacy, and increased control over data. In Web3, the concept of a trustless system comes to the fore, with cryptographic guarantees replacing the need for intermediaries. The economic inclusivity that Web3 can potentially offer, facilitated by blockchain technology and cryptocurrencies, also represents a significant step forward.

Yet, the transition to Web3 is not straightforward and is fraught with challenges. Technical complexities, scalability issues, regulatory uncertainties, and a general lack of