

Contents

Part I Blockchain Fundamentals

1 Blockchain Foundations	3
1.1 Introduction	3
1.1.1 Terminology	4
1.1.2 The First Use Case	4
1.1.3 Currencies: Traditional and Crypto	6
1.1.4 Ownership	7
1.2 Cryptocurrencies	9
1.2.1 Control Mechanisms	9
1.2.2 Cryptography	9
1.2.3 Cryptographic Hashing	9
1.2.4 Asymmetric Cryptography	10
1.2.5 Digital Signatures	11
1.3 Network Architecture Basics	11
1.4 The Blockchain	12
1.4.1 Operations	12
1.4.2 Blocks	12
1.5 Data Integrity	15
1.5.1 Ledger Propagation	15
1.5.2 Transaction Validation	15
1.5.3 Merkle Trees	17
1.6 Types of Blockchains	18
1.6.1 Public Blockchains	18
1.6.2 Private Blockchains	18
1.6.3 Consortium-Controlled Blockchains	19
1.6.4 Selection Framework	19
1.7 Exercise	20
1.7.1 Introduction	20
1.7.2 Environment Setup	20
1.7.3 Build Your Own Blockchain	21
References	27

2	Cryptocurrencies	29
2.1	Introduction	29
2.1.1	Overview	30
2.1.2	Crypto Properties	30
2.1.3	Transactions	31
2.1.4	Double Spending	32
2.2	Miners	33
2.2.1	Process Overview	33
2.2.2	Transaction Confirmation	34
2.2.3	Mining Process	35
2.2.4	The Nonce	36
2.3	Coins and Tokens	37
2.3.1	Introduction	37
2.3.2	Altcoins	38
2.3.3	Tokens	38
2.3.4	ERC-20 Standard	39
2.4	Market Makers/Exchanges	40
2.4.1	Introduction	40
2.4.2	Brokers	41
2.4.3	Traditional Exchanges	42
2.4.4	Decentralized Exchanges	42
2.4.5	Trading Platforms	42
2.4.6	Offline Exchanges	43
2.5	Wallets	43
2.5.1	Introduction	43
2.5.2	Hardware Wallets	43
2.5.3	Software Wallets	44
2.5.4	Exchange Wallets	44
2.6	Exercise	45
2.6.1	Introduction	45
2.6.2	Standard Transfer	45
	References	51
3	Consensus Mechanisms	53
3.1	Introduction	53
3.1.1	Definition	53
3.1.2	Objectives	54
3.1.3	Variations	55
3.2	The CAP Theorem	55
3.2.1	The Trilemma	55
3.2.2	CAP Theorem and Blockchains	56
3.2.3	CAP Theorem in Practice	57

3.3	Byzantine Fault	59
3.3.1	Background	59
3.3.2	Byzantine Generals' Problem	59
3.3.3	An Example	60
3.4	Common Consensus Protocols	61
3.4.1	Proof of Work (PoW)	62
3.4.2	Proof of Stake (PoS)	63
3.4.3	Proof of Capacity/Proof of Space	64
3.4.4	Delegated Proof of Stake (DPoS)	65
3.4.5	Proof of Authority (PoA)	66
3.4.6	Practical Byzantine Fault Tolerance (PBFT)	67
3.4.7	Proof of Elapsed Time (PoET)	68
3.4.8	Other Mechanisms	69
3.5	Exercise	69
3.5.1	Introduction	69
3.5.2	Set up PoA Genesis Block	70
3.5.3	Create a PoA Network	72
	References	73
4	Smart Contracts	75
4.1	Introduction	75
4.2	Ethereum—An Alternative to Bitcoin	77
4.2.1	Introduction	77
4.2.2	Ethereum Versus Bitcoin Applications	77
4.2.3	Ethereum Approach	79
4.2.4	Gas	80
4.2.5	The Price of Gas	81
4.3	Solidity Programming Language	81
4.3.1	Syntax	82
4.3.2	Coin Toss Example	82
4.4	Oracles	83
4.4.1	Introduction	83
4.4.2	Smart Contract Integration	84
4.4.3	Oracles and Security	84
4.4.4	Types of Oracles	85
4.4.5	Oracle Contract Example	85
4.5	Decentralized Applications (dApps)	86
4.5.1	Introduction	86
4.5.2	dApp Example: The Decentralized Autonomous Organization (DAO)	87
4.6	Turing Completeness	88
4.6.1	Background	88
4.6.2	Turing Completeness and Ethereum	88

4.7	Legal Perspective	89
4.7.1	Smart Contract Interpretation	89
4.7.2	Open Questions	90
4.7.3	Conclusion	90
4.8	Exercise (“Piggy Bank”)	91
4.8.1	Introduction	91
4.8.2	Opcode	91
4.8.3	Bytecode	92
4.8.4	Application Binary Interface (ABI)	92
4.8.5	Piggy Bank Deployment	93
	References	97
5	Privacy and Anonymity	99
5.1	Introduction	99
5.1.1	Anonymity	100
5.1.2	Unlinkability	100
5.1.3	Anonymity Versus Pseudonymity	100
5.1.4	Taint Analysis	102
5.2	De-anonymization	103
5.2.1	Introduction	103
5.2.2	Transaction Graph Analysis	103
5.2.3	Network-Layer De-anonymization	103
5.3	The Onion Router (TOR) Network	104
5.3.1	Background	104
5.3.2	TOR Approach	104
5.3.3	TOR Usage	105
5.3.4	Limitations	106
5.4	Mixing Models	106
5.5	Decentralized Mixing	107
5.5.1	Motivation	107
5.5.2	Coinjoin Model	107
5.5.3	Coinjoin Anonymity	108
5.6	Zero-Knowledge Proofs	109
5.6.1	Introduction	109
5.7	Privacy and Security Protocols	110
5.7.1	Introduction	110
5.8	Privacy Coins	111
5.8.1	Introduction	111
5.8.2	The Zero Currencies	112
5.8.3	Zerocoin	113
5.8.4	Zerocash	115
5.9	Exercise	116
5.9.1	Introduction	116
	References	121

Part II Cryptography Foundations

6 Blockchain Cryptography: Part 1 125

6.1 Introduction 125

6.1.1 Cryptography Fundamentals 125

6.1.2 Secrecy Prerequisites 126

6.1.3 Blockchain and Cryptography 126

6.2 Classic Ciphers 127

6.2.1 Substitution 127

6.2.2 Transposition 128

6.3 Modern Cryptographic Algorithms 129

6.3.1 Introduction 129

6.3.2 Vulnerabilities 131

6.4 Hashing 131

6.4.1 Introduction 131

6.4.2 Hash Collisions 132

6.4.3 Merkle-Damgård Construction 133

6.4.4 Length Extension Attack 133

6.5 Secure Hash Algorithm (SHA) 134

6.5.1 Introduction 134

6.5.2 Hash Example 135

6.6 Symmetric Encryption 136

6.6.1 Single Encryption Keys 136

6.6.2 The Hill Cipher 137

6.6.3 The Pohlig-Hellman Cipher 141

6.7 Exercise 144

6.7.1 Introduction 144

6.7.2 Message Prep 144

6.7.3 OpenSSL Setup 145

6.7.4 Message Encryption 145

6.7.5 Message Decryption 147

References 147

7 Blockchain Cryptography: Part 2 149

7.1 Asymmetric Key Schemes 149

7.1.1 Introduction 149

7.1.2 Illustrative Example 150

7.2 Diffie-Hellman-Merkle Key Agreement 151

7.2.1 Introduction 151

7.2.2 An Example 152

7.2.3 Limitations 154

7.3 Rivest, Shamir, and Adelman (RSA) 154

7.3.1 Introduction 154

7.3.2 Key Pairs 155

7.3.3	Intuition	157
7.3.4	An Example	158
7.4	Digital Signatures	159
7.4.1	Introduction	159
7.4.2	Motivation	159
7.4.3	Usage	160
7.4.4	Signatures	160
7.4.5	An Example	162
7.5	Quantum Resistance	163
7.5.1	Introduction	163
7.5.2	Mechanism	163
7.5.3	Shor's Algorithm	164
7.5.4	Grover's Algorithm	164
7.5.5	Imminence	165
7.5.6	Security Considerations	165
7.5.7	Quantum Resistance	165
7.6	Exercise	165
7.6.1	Introduction	165
7.6.2	Message Prep	166
7.6.3	Key Generation (RSA)	166
7.6.4	Digital Signatures (RSA)	168
7.6.5	Key Generation (Elliptic Curves)	168
7.6.6	Digital Signatures (Elliptic Curves)	169
	References	170

Part III Real-World Applications

8	Blockchain in Action: Real-World Applications	173
8.1	Introduction	173
8.2	Currencies	174
8.3	Cross-Border Transfers	175
8.4	Tokenization	176
8.5	Asset Tracking	177
8.6	Commodity Trading	178
8.7	Looking Ahead	179
8.7.1	Humble Beginnings	179
8.7.2	A Word of Caution	180
8.7.3	The Jury Is Still Out	181
	References	183
	Index	185