

Contents

<i>Foreword</i>	xiii
<i>Preface</i>	xv
<i>Acknowledgments</i>	xvii
1. Introduction	1
1.1 Book Structure	2
2. Preliminaries	5
2.1 Basics of Number Theory	5
2.1.1 Divisibility and Greatest Common Divisors	6
2.1.2 Prime Numbers, Relatively Prime Numbers, and Unique Factorization	7
2.1.3 Euler's Totient Function $\varphi(n)$	9
2.2 Algebraic Foundations	13
2.2.1 Modular Arithmetic	13
2.2.1.1 Congruences	14
2.2.1.2 Residue Classes	15
2.2.2 Groups	18
2.2.2.1 Binary Operators	18
2.2.2.2 The Group Axioms	19
2.2.2.3 Elementary Properties	21
2.2.2.4 Group Homomorphisms, Isomorphisms, and Endomorphisms	22
2.2.2.5 Subgroups	24
2.2.2.6 Order of Groups and Elements	25
2.2.2.7 Cyclic Groups	27
2.2.2.8 The Group of Units in the Integers modulo n	34
2.2.2.9 The Euler–Fermat Theorem	37
2.2.3 Rings	38
2.2.3.1 Definition of a Ring	39
2.2.3.2 The Residue Class Ring \mathbb{Z}_n	40
2.2.3.3 Units and Zero Divisors	41
2.2.3.4 Integral Domains	42
2.2.4 Fields	43
2.2.4.1 Definition of a Field	43
2.2.4.2 Properties of Fields	44
2.2.5 Finite Fields	46
2.2.5.1 Existence and Uniqueness	46
2.2.5.2 Basic Properties	47

2.2.5.3	Prime Fields	48
2.2.5.4	The Multiplicative Group \mathbb{F}_q^* and Primitive Roots	48
2.3	Computational Complexity	51
2.3.1	Introduction	51
2.3.2	Asymptotic Order of Growth	51
2.3.2.1	\mathcal{O} , Ω , and Θ	52
2.3.3	Classes of Time Complexity	54
2.3.4	Efficiency of Algorithms	55
3.	Cryptographic Primitives	57
3.1	Introduction	57
3.2	Cryptography Basics	58
3.2.1	Basic Communication Model	58
3.2.2	Basic Cryptosystem	60
3.2.3	Symmetric vs. Asymmetric (Public-Key) Cryptography	61
3.3	Public-Key Cryptography	63
3.3.1	One-Way and Trapdoor Functions	65
3.3.2	Basic Functionality of a Public-Key Cryptosystem	66
3.3.2.1	Key Generation	66
3.3.2.2	Key Exchange and Secure Communication	67
3.3.2.3	Authenticated Messaging	68
3.3.2.4	Digital Signatures	69
3.3.3	The Diffie–Hellman Key Exchange	72
3.3.4	The Discrete Logarithm Problem	74
3.3.4.1	The DLP in \mathbb{F}_p^*	74
3.3.4.2	The Generalized Discrete Logarithm Problem	75
3.3.4.3	Attacks Against DLPs	76
3.4	Hash Functions	77
3.4.1	Introduction	77
3.4.2	Properties of Hash Functions	78
3.4.3	Security of Hash Functions and the Birthday Attack	80
3.4.4	Real Hash Functions	84
3.4.4.1	Classification of Hash Functions	84
3.4.4.2	The Merkle–Damgård Construction	84
3.4.4.3	Structural Weakness	88
3.4.4.4	Security of Real-Life Dedicated Hash Functions	89
3.5	Merkle Trees	91
3.6	Elliptic Curve Cryptography	92
3.6.1	Weierstrass Equations	93
3.6.2	Elliptic Curves	95
3.6.2.1	Definition	95
3.6.2.2	The j -Invariant	95
3.6.2.3	Group Law	96
3.6.3	Elliptic Curves over Finite Fields	102
3.6.3.1	Examples of Elliptic Curves over \mathbb{F}_p	103
3.6.3.2	Addition of Points	105

3.6.3.3	Order of Points	106
3.6.3.4	Group Order	106
3.6.3.5	Group Structure	108
3.6.3.6	Special Curves	109
3.6.4	The Elliptic Curve Discrete Logarithm Problem	109
3.6.4.1	Definition	109
3.6.4.2	A First Application of ECDLP: ECDH	110
3.6.4.3	Attacking the ECDLP	111
3.6.5	Cryptographically Secure Elliptic Curves	115
3.6.5.1	Domain Parameters	116
3.6.5.2	Requirements on Cryptographically Strong EC Domain Parameters	116
3.6.5.3	Additional (Security) Requirements	117
3.6.5.4	Recommended Elliptic Curves by Standards	122
3.6.5.5	The Elliptic Curve secp256k1	124
3.6.6	The Elliptic Curve Digital Signature Algorithm	127
3.6.6.1	Key Pair Generation	127
3.6.6.2	Public Key Validation	128
3.6.6.3	ECDSA Signature Generation and Validation	128
3.6.6.4	Attacks on ECDSA	130
4.	Information Security in Software Systems	135
4.1	Introduction	135
4.2	The CIA Triad	135
4.3	Attacks Against Distributed Systems	138
4.3.1	Denial-of-Service (DoS) Attack	138
4.3.2	Sybil Attack	138
4.4	Proof-of-Work	139
5.	Distributed Systems	143
5.1	Introduction	143
5.2	Classification of Systems	143
5.2.1	Centralized Systems	147
5.2.2	Decentralized Systems	148
5.2.3	Distributed Systems	149
5.2.3.1	Definition	149
5.2.3.2	CAP Theorem	151
5.2.3.3	Fault Tolerance	153
5.2.3.4	Peer-to-Peer Systems	154
5.2.4	Summary	155
5.3	Reaching Consensus in Distributed Systems	155
5.3.1	Introduction	155
5.3.2	Consensus and Agreement	156
5.3.3	Consensus and Fault Tolerance	157
5.3.4	Models of Computation	159
5.3.4.1	Failure Model	160
5.3.4.2	Interaction Model	162

5.3.4.3	Security Model: Signatures	164
5.3.4.4	Adversary Model	165
5.3.5	Consensus and Agreement Protocols	166
5.3.5.1	Types of Algorithms	166
5.3.5.2	Basic Properties of Consensus Protocols	168
5.3.5.3	Agreement Algorithms for Synchronous Systems	170
5.3.6	Agreement in a Failure-Free System	171
5.3.7	Consensus with Crash Failures in Synchronous Systems	172
5.3.7.1	Problem Definition	172
5.3.7.2	Consensus Algorithms for Crash Failures (Synchronous System)	173
5.3.8	Byzantine Agreement in Synchronous Systems	179
5.3.8.1	The Byzantine Generals Problem	179
5.3.8.2	Problem Definition	182
5.3.8.3	Agreement Algorithms for Byzantine Failures (Synchronous System)	183
5.3.9	Agreement in Asynchronous Systems	186
5.3.9.1	Impossibility in Asynchronous Systems	187
5.3.9.2	Circumventing the FLP Impossibility Result	188
5.3.9.3	Practical Solutions	195
5.3.10	Summary	196
6.	Introduction to Blockchain Technology	199
6.1	Introduction	199
6.2	Definition of Blockchain	200
6.3	PoW vs. BFT Blockchains	200
6.4	Blockchain as a Suite of Technologies	202
6.4.1	Blockchain Network	202
6.4.2	Ordering Transactions in a Blockchain	203
6.4.3	Implementing State Replication by Using Blockchain	205
6.4.4	Reaching Consensus on the Network	206
6.4.4.1	Creating New Blocks for the Authoritative Chain	207
6.4.4.2	Transaction Lifecycle	209
6.4.4.3	Resolving Forks Using the Longest-Chain-Criterion	210
6.4.4.4	Acceptance of New Blocks	213
6.5	The Blockchain as a Data Structure	215
6.5.1	Aggregating Transactions	216
6.5.2	Structure of a Block	216
6.5.3	The Blockchain	218
6.5.4	Tamper-Proof Ledgers	220
6.6	Information Security in Blockchain Systems	222
6.7	Proof-of-Work	223
6.7.1	Partial Hash Inversion	223
6.7.2	Proof-of-Work in Blockchain Systems	225

6.8	The Double-Spending Attack	226
6.8.1	The Double-Spending Problem	227
6.8.2	Confirmation Security	227
6.8.3	Transaction Commitment	229
6.8.4	The General Double-Spending Attack: The Race Attack	230
6.8.4.1	Setting Up a Double-Spending Attack	230
6.8.4.2	Probability of a Successful Double-Spending Attack	231
6.8.4.3	Specific Cases	234
6.8.5	Other Attacks	235
6.8.5.1	51% Attack	235
6.8.5.2	Finney Attack	235
6.8.5.3	Transaction Spamming	236
6.8.5.4	Eclipse Attack	237
6.9	The Incentive System of the Nakamoto Consensus	237
6.9.1	The Incentive System as a Countermeasure Against Double-Spending Attacks	237
6.9.2	Selfish Mining	238
6.9.3	Security of the Nakamoto Consensus Protocol	238
6.10	Summary	239
7.	Bitcoin	241
7.1	Introduction	241
7.2	System Basics	243
7.3	Keys and Addresses	244
7.4	Transactions	245
7.4.1	Inputs and Outputs	247
7.4.2	The Transaction Script	250
7.4.2.1	Script Language	250
7.4.2.2	Transaction Validation: Locking and Unlocking Script	251
7.4.2.3	Standard Transaction Script Pay-To-Public-Key-Hash (P2PKH)	251
7.4.3	Storing the Transactions in the Blockchain	255
7.4.4	Transaction Lifecycle in Bitcoin	255
7.5	The Blockchain	256
7.5.1	The Block Header	256
7.5.2	Solving the Proof-of-Work	257
7.6	Summary	258
8.	Introduction to Quantum Computing	259
8.1	Introduction	259
8.2	Definition of a Quantum Bit	259
8.2.1	Comparison to Classical Bits	259
8.2.2	Mathematical Representation of a Qubit	260
8.3	Quantum Computation Algorithms	261
8.3.1	Grover's Algorithm	261
8.3.2	Shor's Algorithm	261

8.4	Impact on Present Cryptography	262
8.5	Summary	263
9.	Bitcoin Under Broken Crypto Primitives	265
9.1	Introduction	265
9.2	A General Overview of the Primitives	265
9.2.1	The Digital Signature Scheme	265
9.2.1.1	Attacks Against the ECDLP	266
9.2.1.2	Attacks Against the Ephemeral Key	267
9.2.2	Hash Functions	267
9.2.2.1	Attacks Against the Address Hash in P2PKH Transactions	268
9.2.2.2	Attacks Against the PoW	269
9.2.2.3	Attacks Against Existing Blocks	270
9.2.2.4	Attacks Against Existing Transactions of the Merkle Tree	270
9.2.3	Combined Attacks	271
9.3	Impact of Quantum Computers	272
9.3.1	Grover's Algorithm	273
9.3.2	Shor's Algorithm	275
9.3.3	Combining Both Grover's and Shor's Algorithms	276
9.4	Summary	276
10.	Post-Quantum Blockchains	279
10.1	Introduction	279
10.2	Post-Quantum Cryptography	280
10.3	Comparison Between Classical and Quantum Safe Schemes	282
10.4	Hash-Based Cryptosystems	285
10.4.1	Lamport-Diffie One-Time Signatures	285
10.4.1.1	Key Generation, Signature Generation, and Verification	286
10.4.2	Multi-Time Signatures	288
10.5	Summary	290
11.	Conclusions	291
	<i>List of Abbreviations</i>	293
	<i>List of Notations</i>	295
	<i>List of Figures</i>	299
	<i>List of Tables</i>	303
	<i>Bibliography</i>	305
	<i>Index</i>	319