1. CHAPTER 1 Introduction to Cryptography and Cryptocurrencies 1
   1. CRYPTOGRAPHIC HASH FUNCTIONS 34
      * Property 1: Collision Resistance
      * Property 2: Hiding
      * Property 3: Puzzle Friendliness
      * SHA-256
   2. HASH POINTERS AND DATA STRUCTURES 45
      * Block Chain
      * Merkle Trees
      * Proof of Membership
      * Proof of Nonmembership
   3. DIGITAL SIGNATURES 50
      * Practical Concerns
      * ECDSA
   4. PUBLIC KEYS AS IDENTITIES 55
      * Decentralized Identity Management
   5. TWO SIMPLE CRYPTOCURRENCIES 58
      * Goofycoin
      * Scroogecoin
   6. FURTHER READING 64
2. CHAPTER 2 How Bitcoin Achieves Decentralization 27
   1. CENTRALIZATION VERSUS DECENTRALIZATION 66
   2. DISTRIBUTED CONSENSUS 68
      * Impossibility Results
      * Breaking Traditional Assumptions
   3. CONSENSUS WITHOUT IDENTITY USING A BLOCK CHAIN 72
      * Implicit Consensus
   4. INCENTIVES AND PROOF OF WORK 24
      * Block Reward
      * Transaction Fees
      * Mining and Proof of Work
      * Difficult to Compute
      * Parameterizable Cost
      * Trivial to Verify
   5. PUTTING IT ALL TOGETHER 88
      * Cost of Mining
      * Getting a Cryptocurrency off the Ground
      * The 51 Percent Attack
   6. FURTHER READING 95
3. CHAPTER 3 Mechanics of Bitcoin 51
   1. BITCOIN TRANSACTIONS 96
   2. BITCOIN SCRIPTS 101
      * Bitcoin Scripting Language
      * Executing a Script
      * What’s Used in Practice
      * Proof of Burn
      * Pay-to-Script-Hash
   3. APPLICATIONS OF BITCOIN SCRIPTS 108
      * Escrow Transactions
      * Green Addresses
      * Efficient Micropayments
      * Lock Time
      * Smart Contracts
   4. BITCOIN BLOCKS 113
   5. THE BITCOIN NETWORK 116
      * Size of the Network
      * Storage Requirements
      * Lightweight Nodes
   6. LIMITATIONS AND IMPROVEMENTS 122
      * Changing the Protocol
   7. FURTHER READING 127
4. CHAPTER 4 How to Store and Use Bitcoins 76
   1. SIMPLE LOCAL STORAGE 128
      * Wallets
      * Encoding Keys: Base 58 and QR Codes
      * Vanity Addresses
   2. HOT AND COLD STORAGE 132
      * Hierarchical Deterministic Wallets
      * Brain Wallet
      * Paper Wallet
      * Tamper-Resistant Device
   3. SPLITTING AND SHARING KEYS 138
      * Threshold Cryptography
      * Multisignatures
   4. ONLINE WALLETS AND EXCHANGES 143
      * Online Wallets
      * Bitcoin Exchanges
      * Three Types of Risks
      * Bank Regulation
      * Proof of Reserve
      * Proof of Liabilities
   5. PAYMENT SERVICES 151
   6. TRANSACTION FEES 156
   7. CURRENCY EXCHANGE MARKETS 158
      * Supply and Demand
      * A Simple Model of Market Behavior
   8. FURTHER READING 163
5. CHAPTER 5 Bitcoin Mining 104
   1. THE TASK OF BITCOIN MINERS 165
      * Finding a Valid Block
      * Determining the Difficulty
   2. MINING HARDWARE 172
      * A Closer Look at SHA-256
      * CPU Mining
      * GPU Mining
      * Disadvantages of GPU Mining
      * Mining with Field-Programmable Gate Arrays
      * Mining with Application-Specific Integrated Circuits
      * Professional Mining Today
      * Similarities to Gold Mining
      * The Future
      * The Cycle Repeats Itself
   3. ENERGY CONSUMPTION AND ECOLOGY 184
      * Thermodynamic Limits
      * Mining at Scale
      * Estimating Energy Usage
      * Is Bitcoin Mining Wasteful?
      * Repurposing Energy
      * Turning Electricity into Cash
   4. MINING POOLS 190
      * High Variance
      * Mining Pools
      * Mining Shares
      * Pay per Share
      * Proportional
      * Pool Hopping
      * History and Standardization
      * 51 Percent Mining Pools
      * Are Mining Pools Beneficial?
   5. MINING INCENTIVES AND STRATEGIES 199
      * Forking Attack
      * Forking Attack via Bribery
      * Forking Attack via Bribery
      * Blacklisting and Punitive Forking
      * Blacklisting and Punitive Forking
      * Open Problems
   6. URTHER READING 206
6. CHAPTER 6 Bitcoin and Anonymity 138
   1. ANONYMITY BASICS 208
      * Defining Anonymity
      * Side Channels
      * Unlinkability
      * Anonymity Set
      * Taint Analysis
      * Why Anonymity Is Needed
      * Ethics of Anonymity
      * Anonymization versus Decentralization
   2. HOW TO DEANONYMIZE BITCOIN 215
      * Linking
      * Idioms of Use
      * Attaching Real-World Identities to Clusters
      * Tagging by Transacting
      * Identifying Individuals
      * Network-Layer Deanonymization
   3. MIXING 225
      * Online Wallets as Mixes
      * Dedicated Mixing Services
      * Guidelines for Mixing
      * Mixing in Practice
   4. DECENTRALIZED MIXING 231
      * CoinJoin
      * High-Level Flows
   5. ZEROCOIN AND ZEROCASH 235
      * Zerocoin
      * Zero-Knowledge Proofs
      * Minting Zerocoins
      * Trusted Setup
      * Zerocash
      * Setting Up Zerocash
      * Putting It All Together
   6. FURTHER READING 244
7. CHAPTER 7 Community, Politics, and Regulation 168
   1. CONSENSUS IN BITCOIN 247
   2. BITCOIN CORE SOFTWARE 249
      * Bitcoin Improvement Proposals
      * Bitcoin Core Developers
      * Forks in the Rules
   3. STAKEHOLDERS: WHO’S IN CHARGE? 253
   4. ROOTS OF BITCOIN 256
      * Cypherpunk and Digital Cash
      * Satoshi Nakamoto
      * Growth
   5. GOVERNMENTS NOTICE BITCOIN 259
      * Capital Controls
      * Crime
      * Silk Road
      * Lessons from Silk Road
   6. ANTI-MONEY LAUNDERING 264
      * Know Your Customer
      * Mandatory Reporting
   7. REGULATION 266
      * Lemons Market
      * Fixing a Lemons Market
      * Regulatory Fixes
      * Collusion and Antitrust Law
   8. NEW YORK’S BITLICENSE 270
      * Who’s Covered
      * Requirements
   9. FURTHER READING 273
8. CHAPTER 8 Alternative Mining Puzzles 190
   1. ESSENTIAL PUZZLE REQUIREMENTS 275
   2. ASIC-RESISTANT PUZZLES 277
      * What Does ASIC Resistance Mean?
      * Memory-Hard Puzzles
      * Scrypt
      * Time-Memory Trade-Offs
      * Verification Cost
      * Scrypt in Practice
      * Other Approaches to ASIC Resistance
      * The ASIC Honeymoon
      * Arguments against ASIC Resistance
   3. PROOF OF USEFUL WORK 285
      * Previous Distributed Computing Projects
      * Primecoin
      * Permacoin and Proof of Storage
      * Long-Term Challenges and Economics
   4. NONOUTSOURCEABLE PUZZLES 292
      * Technical Requirements for Pools
      * Block-Discarding Attacks
      * Rewarding Sabotage
      * Pros and Cons of Nonoutsourceable Mining
   5. PROOF OF STAKE AND VIRTUAL MINING 296
      * Closing the Loop on Mining
      * Advantages of Virtual Mining
      * Implementing Virtual Mining: Peercoin
      * Alternate Forms of Stake
      * The Nothing-at-Stake Problem
      * Other Drawbacks of Virtual Mining
      * Can Virtual Mining Actually Work?
   6. FURTHER READING 302
9. CHAPTER 9 Bitcoin as a Platform 213
   1. BITCOIN AS AN APPEND-ONLY LOG 304
      * Secure Timestamping
      * Applications of Timestamping
      * Attacks on Proofs of “Clairvoyance”
      * Secure Timestamping the Old-Fashioned Way
      * Secure Timestamping in Bitcoin
      * Unspendable Outputs
      * Illicit Content
      * Overlay Currencies
   2. BITCOINS AS “SMART PROPERTY” 312
      * Smart Property
      * Colored Coins
      * OpenAssets
      * Uses of Colored Coins and Smart Property
   3. SECURE MULTIPARTY LOTTERIES IN BITCOIN 318
      * Coin Flipping Online
      * Fairness
   4. BITCOIN AS A PUBLIC RANDOMNESS SOURCE 322
      * NBA Draft Lottery
      * U.S. Military Draft Lottery
      * Cryptographic Beacons
      * National Institute of Standards and Technology Beacon
      * Other Potential Ways to Build a Beacon: Natural Phenomena
      * Financial Data
      * Using Bitcoin as a Beacon
      * Evaluating the Security of a Bitcoin Beacon
      * Scripting Support for Beacons
   5. PREDICTION MARKETS AND REAL-WORLD DATA FEEDS
      * Decentralized Prediction Markets
      * Payment and Settlement
      * Prediction Market Arbitration
      * Data Feeds
      * Order Books
   6. FURTHER READING 340
10. CHAPTER 10 Altcoins and the Cryptocurrency Ecosystem 242
    1. ALTCOINS: HISTORY AND MOTIVATION 342
       * Reasons for Launching Altcoins
       * How to Launch an Altcoin
       * Pump-and-Dump Scams
       * Initial Allocation
    2. A FEW ALTCOINS IN DETAIL 348
       * Namecoin
       * Litecoin
       * Dogecoin
    3. RELATIONSHIP BETWEEN BITCOIN AND ALTCOINS 352
       * Comparing Altcoins
       * Economic View of Bitcoin-Altcoin Interactions
    4. ALTCOIN INFANTICIDE AND MERGE MINING 355
       * Altcoin Infanticide
       * Merge Mining
       * Merge Mining and Security
    5. ATOMIC CROSS-CHAIN SWAPS 361
    6. SIDECHAINS: BITCOIN-BACKED ALTCOINS 364
       * The SPV Trick
       * Contesting a Transfer
       * Compact SPV Proofs via Proof-of-Work Samples
    7. ETHEREUM AND SMART CONTRACTS 368
       * Smart Contract Programming Model
       * A Simple Example: Namecoin in Ethereum
       * Gas, Incentives, and Security
       * A Second Example: Chess in Ethereum
       * Other Applications
       * Ethereum Project
    8. FURTHER READING 378
11. CHAPTER 11 Decentralized Institutions: The Future of Bitcoin? 272
    1. THE BLOCK CHAIN AS A VEHICLE FOR DECENTRALIZATION 380
       * Motivating Example
       * Get Smart
       * Secure Exchange
    2. ROUTES TO BLOCK CHAIN INTEGRATION 383
       * Route 1: Directly on Bitcoin
       * Route 2: Alternative Block Chains
    3. TEMPLATE FOR DECENTRALIZATION 388
       * Levels of Decentralization
       * How Security Is Achieved
       * The Framework
    4. WHEN IS DECENTRALIZATION A GOOD IDEA? 393
       * The Challenge of Real-World Security
       * Pros and Cons of Smart Property
       * Crypto, the State, and the Big Opportunity

CONCLUSION 286

ACKNOWLEDGMENTS 287

ABOUT THE AUTHORS 289