

Table of Contents

Preface.....	xiii
Quick Glossary.....	xxv
1. Introduction.....	1
What Is Bitcoin?	1
History of Bitcoin	4
Bitcoin Uses, Users, and Their Stories	5
Getting Started	6
Choosing a Bitcoin Wallet	6
Quick Start	8
Getting Your First Bitcoin	10
Finding the Current Price of Bitcoin	11
Sending and Receiving Bitcoin	12
2. How Bitcoin Works.....	15
Transactions, Blocks, Mining, and the Blockchain	15
Bitcoin Overview	15
Buying a Cup of Coffee	16
Bitcoin Transactions	18
Transaction Inputs and Outputs	18
Transaction Chains	19
Making Change	20
Common Transaction Forms	21
Constructing a Transaction	22
Getting the Right Inputs	22
Creating the Outputs	24
Adding the Transaction to the Ledger	25
Bitcoin Mining	26
Mining Transactions in Blocks	27

Spending the Transaction	29
3. Bitcoin Core: The Reference Implementation.....	31
Bitcoin Development Environment	32
Compiling Bitcoin Core from the Source Code	32
Selecting a Bitcoin Core Release	33
Configuring the Bitcoin Core Build	34
Building the Bitcoin Core Executables	36
Running a Bitcoin Core Node	38
Configuring the Bitcoin Core Node	39
Bitcoin Core Application Programming Interface (API)	43
Getting Information on the Bitcoin Core Client Status	44
Exploring and Decoding Transactions	45
Exploring Blocks	47
Using Bitcoin Core's Programmatic Interface	48
Alternative Clients, Libraries, and Toolkits	52
C/C++	52
JavaScript	52
Java	52
PHP	53
Python	53
Ruby	53
Go	53
Rust	53
C#	53
Objective-C	53
4. Keys, Addresses.....	55
Introduction	55
Public Key Cryptography and Cryptocurrency	56
Private and Public Keys	57
Private Keys	58
Public Keys	60
Elliptic Curve Cryptography Explained	60
Generating a Public Key	63
Bitcoin Addresses	64
Base58 and Base58Check Encoding	66
Key Formats	69
Implementing Keys and Addresses in C++	75
Implementing Keys and Addresses in Python	77
Advanced Keys and Addresses	80
Encrypted Private Keys (BIP-38)	80

Pay-to-Script Hash (P2SH) and Multisig Addresses	81
Vanity Addresses	83
Paper Wallets	88
5. Wallets	93
Wallet Technology Overview	93
Nondeterministic (Random) Wallets	94
Deterministic (Seeded) Wallets	95
HD Wallets (BIP-32/BIP-44)	96
Seeds and Mnemonic Codes (BIP-39)	97
Wallet Best Practices	97
Using a Bitcoin Wallet	98
Wallet Technology Details	99
Mnemonic Code Words (BIP-39)	99
Creating an HD Wallet from the Seed	106
Using an Extended Public Key on a Web Store	110
6. Transactions	117
Introduction	117
Transactions in Detail	117
Transactions—Behind the Scenes	118
Transaction Outputs and Inputs	119
Transaction Outputs	121
Transaction Inputs	123
Transaction Fees	126
Adding Fees to Transactions	129
Transaction Scripts and Script Language	131
Turing Incompleteness	131
Stateless Verification	132
Script Construction (Lock + Unlock)	132
Pay-to-Public-Key-Hash (P2PKH)	136
Digital Signatures (ECDSA)	138
How Digital Signatures Work	139
Verifying the Signature	141
Signature Hash Types (SIGHASH)	141
ECDSA Math	143
The Importance of Randomness in Signatures	145
Bitcoin Addresses, Balances, and Other Abstractions	145
7. Advanced Transactions and Scripting	149
Introduction	149
Multisignature	149

Pay-to-Script-Hash (P2SH)	151
P2SH Addresses	154
Benefits of P2SH	155
Redeem Script and Validation	155
Data Recording Output (RETURN)	156
Timelocks	157
Transaction Locktime (nLocktime)	158
Check Lock Time Verify (CLTV)	159
Relative Timelocks	161
Relative Timelocks with nSequence	161
Relative Timelocks with CSV	163
Median-Time-Past	163
Timelock Defense Against Fee Sniping	164
Scripts with Flow Control (Conditional Clauses)	165
Conditional Clauses with VERIFY Opcodes	166
Using Flow Control in Scripts	167
Complex Script Example	168
Segregated Witness	170
Why Segregated Witness?	171
How Segregated Witness Works	172
Soft Fork (Backward Compatibility)	173
Segregated Witness Output and Transaction Examples	173
Upgrading to Segregated Witness	176
Segregated Witness' New Signing Algorithm	182
Economic Incentives for Segregated Witness	183
8. The Bitcoin Network	187
Peer-to-Peer Network Architecture	187
Node Types and Roles	188
The Extended Bitcoin Network	189
Bitcoin Relay Networks	192
Network Discovery	192
Full Nodes	196
Exchanging "Inventory"	197
Simplified Payment Verification (SPV) Nodes	199
Bloom Filters	201
How Bloom Filters Work	202
How SPV Nodes Use Bloom Filters	205
SPV Nodes and Privacy	206
Encrypted and Authenticated Connections	207
Tor Transport	207
Peer-to-Peer Authentication and Encryption	207

Transaction Pools	208
9. The Blockchain	211
Introduction	211
Structure of a Block	212
Block Header	213
Block Identifiers: Block Header Hash and Block Height	213
The Genesis Block	214
Linking Blocks in the Blockchain	216
Merkle Trees	217
Merkle Trees and Simplified Payment Verification (SPV)	223
Bitcoin's Test Blockchains	223
Testnet—Bitcoin's Testing Playground	224
Segnet—The Segregated Witness Testnet	225
Regtest—The Local Blockchain	225
Using Test Blockchains for Development	226
10. Mining and Consensus	229
Introduction	229
Bitcoin Economics and Currency Creation	231
Decentralized Consensus	233
Independent Verification of Transactions	234
Mining Nodes	235
Aggregating Transactions into Blocks	236
The Coinbase Transaction	237
Coinbase Reward and Fees	239
Structure of the Coinbase Transaction	240
Coinbase Data	241
Constructing the Block Header	243
Mining the Block	244
Proof-of-Work Algorithm	244
Target Representation	251
Retargeting to Adjust Difficulty	251
Successfully Mining the Block	253
Validating a New Block	254
Assembling and Selecting Chains of Blocks	255
Blockchain Forks	257
Mining and the Hashing Race	264
The Extra Nonce Solution	266
Mining Pools	267
Consensus Attacks	270
Changing the Consensus Rules	273

Hard Forks	274
Hard Forks: Software, Network, Mining, and Chain	275
Diverging Miners and Difficulty	276
Contentious Hard Forks	277
Soft Forks	278
Criticisms of Soft Forks	279
Soft Fork Signaling with Block Version	280
BIP-34 Signaling and Activation	280
BIP-9 Signaling and Activation	281
Consensus Software Development	283
11. Bitcoin Security	285
Security Principles	285
Developing Bitcoin Systems Securely	286
The Root of Trust	287
User Security Best Practices	288
Physical Bitcoin Storage	289
Hardware Wallets	289
Balancing Risk	289
Diversifying Risk	290
Multisig and Governance	290
Survivability	290
Conclusion	290
12. Blockchain Applications	291
Introduction	291
Building Blocks (Primitives)	292
Applications from Building Blocks	294
Colored Coins	294
Using Colored Coins	295
Issuing Colored Coins	296
Colored Coins Transactions	296
Counterparty	299
Payment Channels and State Channels	300
State Channels—Basic Concepts and Terminology	301
Simple Payment Channel Example	302
Making Trustless Channels	305
Asymmetric Revocable Commitments	308
Hash Time Lock Contracts (HTLC)	312
Routed Payment Channels (Lightning Network)	313
Basic Lightning Network Example	314
Lightning Network Transport and Routing	318

Lightning Network Benefits	320
Conclusion	321
A. The Bitcoin Whitepaper by Satoshi Nakamoto.....	323
B. Transaction Script Language Operators, Constants, and Symbols.....	335
C. Bitcoin Improvement Proposals.....	341
D. Bitcore.....	349
E. pycoin, ku, and tx.....	353
F. Bitcoin Explorer (bx) Commands.....	363
Index.....	367

...and I ignored it for another six months. During that time, I was reading a lot of books and articles about Bitcoin. This is a reaction that I have seen repeated among many of the smartest people I know, which gives me some consolation. The second time I came across the Bitcoin whitepaper, I decided to read the whitepaper, written by Satoshi Nakamoto. I read it and was blown away. I saw the future of money and I saw the future of the world. I saw a digital currency that could be used anywhere, anytime, and I saw a network of trust that could provide a secure and transparent way to transact. The realization that "this is the future" started me on a four-month journey to devour everything I could find about Bitcoin. I read every book, article, and whitepaper I could find. I spent 11 or more hours each day glued to a screen, reading, writing, coding, and working as much as I could. I emerged from this state of hyper-focus more than 20 pounds lighter from lack of consistent meals, determined to dedicate myself to working on Bitcoin.

After a few months of reading a number of small startups to explore various blockchain-related services and products, I decided that it was time to write my first book. Bitcoin was the topic that had driven me into a frenzy of creativity and consumed my thoughts. It was the most exciting technology I had encountered since the Internet. It was time to share my passion about this amazing technology with a broader audience.

Intended Audience

This book is primarily intended for coders. If you can use a programming language, this book will teach you how cryptographic currencies work, how to use them, and how to develop software that works with them. The first few chapters are also suitable as