
Table of Contents

Preface	xi
Quick Glossary	xix
1. Introduction	1
What Is Bitcoin?	1
History of Bitcoin	3
Bitcoin Uses, Users, and Their Stories	4
Getting Started	6
Quick Start	7
Getting Your First Bitcoins	9
Sending and Receiving Bitcoins	10
2. How Bitcoin Works	15
Transactions, Blocks, Mining, and the Blockchain	15
Bitcoin Overview	16
Buying a Cup of Coffee	16
Bitcoin Transactions	18
Common Transaction Forms	20
Constructing a Transaction	21
Getting the Right Inputs	22
Creating the Outputs	23
Adding the Transaction to the Ledger	24
Bitcoin Mining	25
Mining Transactions in Blocks	27
Spending the Transaction	28
3. The Bitcoin Client	31
Bitcoin Core: The Reference Implementation	31
Running Bitcoin Core for the First Time	32

Compiling Bitcoin Core from the Source Code	33
Using Bitcoin Core's JSON-RPC API from the Command Line	39
Getting Information on the Bitcoin Core Client Status	40
Wallet Setup and Encryption	41
Wallet Backup, Plain-text Dump, and Restore	42
Wallet Addresses and Receiving Transactions	43
Exploring and Decoding Transactions	44
Exploring Blocks	48
Creating, Signing, and Submitting Transactions Based on Unspent Outputs	50
Alternative Clients, Libraries, and Toolkits	56
Libbitcoin and sx Tools	57
pycoin	57
btcd	59
4. Keys, Addresses, Wallets.....	61
Introduction	61
Public Key Cryptography and Cryptocurrency	62
Private and Public Keys	63
Private Keys	63
Public Keys	65
Elliptic Curve Cryptography Explained	65
Generating a Public Key	68
Bitcoin Addresses	70
Base58 and Base58Check Encoding	72
Key Formats	76
Implementing Keys and Addresses in Python	81
Wallets	84
Nondeterministic (Random) Wallets	85
Deterministic (Seeded) Wallets	85
Mnemonic Code Words	86
Hierarchical Deterministic Wallets (BIP0032/BIP0044)	87
Advanced Keys and Addresses	97
Encrypted Private Keys (BIP0038)	97
Pay-to-Script Hash (P2SH) and Multi-Sig Addresses	98
Vanity Addresses	99
Paper Wallets	104
5. Transactions.....	109
Introduction	109
Transaction Lifecycle	109
Creating Transactions	110
Broadcasting Transactions to the Bitcoin Network	110

Propagating Transactions on the Bitcoin Network	111
Transaction Structure	111
Transaction Outputs and Inputs	112
Transaction Outputs	113
Transaction Inputs	115
Transaction Fees	118
Adding Fees to Transactions	119
Transaction Chaining and Orphan Transactions	120
Transaction Scripts and Script Language	121
Script Construction (Lock + Unlock)	122
Scripting Language	123
Turing Incompleteness	126
Stateless Verification	126
Standard Transactions	126
Pay-to-Public-Key-Hash (P2PKH)	127
Pay-to-Public-Key	128
Multi-Signature	129
Data Output (OP_RETURN)	130
Pay-to-Script-Hash (P2SH)	132
6. The Bitcoin Network.....	137
Peer-to-Peer Network Architecture	137
Nodes Types and Roles	138
The Extended Bitcoin Network	139
Network Discovery	142
Full Nodes	145
Exchanging “Inventory”	146
Simplified Payment Verification (SPV) Nodes	147
Bloom Filters	150
Bloom Filters and Inventory Updates	155
Transaction Pools	156
Alert Messages	157
7. The Blockchain.....	159
Introduction	159
Structure of a Block	160
Block Header	160
Block Identifiers: Block Header Hash and Block Height	161
The Genesis Block	162
Linking Blocks in the Blockchain	163
Merkle Trees	164
Merkle Trees and Simplified Payment Verification (SPV)	170

8. Mining and Consensus.....	173
Introduction	173
Bitcoin Economics and Currency Creation	174
Decentralized Consensus	176
Independent Verification of Transactions	177
Mining Nodes	179
Aggregating Transactions into Blocks	179
Transaction Age, Fees, and Priority	180
The Generation Transaction	182
Coinbase Reward and Fees	183
Structure of the Generation Transaction	184
Coinbase Data	185
Constructing the Block Header	187
Mining the Block	188
Proof-Of-Work Algorithm	188
Difficulty Representation	194
Difficulty Target and Retargeting	195
Successfully Mining the Block	197
Validating a New Block	197
Assembling and Selecting Chains of Blocks	198
Blockchain Forks	199
Mining and the Hashing Race	204
The Extra Nonce Solution	206
Mining Pools	207
Consensus Attacks	210
9. Alternative Chains, Currencies, and Applications.....	215
A Taxonomy of Alternative Currencies and Chains	216
Meta Coin Platforms	216
Colored Coins	217
Mastercoin	218
Counterparty	218
Alt Coins	218
Evaluating an Alt Coin	219
Monetary Parameter Alternatives: Litecoin, Dogecoin, Freicoin	220
Consensus Innovation: Peercoin, Myriad, Blackcoin, Vericoin, NXT	221
Dual-Purpose Mining Innovation: Primecoin, Curecoin, Gridcoin	223
Anonymity-Focused Alt Coins: CryptoNote, Bytecoin, Monero, Zerocash/ Zerocoin, Darkcoin	225
Noncurrency Alt Chains	226
Namecoin	226
Bitmessage	228

Ethereum	229
Future of Currencies	229
10. Bitcoin Security	231
Security Principles	231
Developing Bitcoin Systems Securely	232
The Root of Trust	233
User Security Best Practices	234
Physical Bitcoin Storage	235
Hardware Wallets	235
Balancing Risk	235
Diversifying Risk	235
Multi-sig and Governance	236
Survivability	236
Conclusion	236
A. Transaction Script Language Operators, Constants, and Symbols	237
B. Bitcoin Improvement Proposals	243
C. pycoin, ku, and tx	247
D. Available Commands with sx Tools	257
Index	263