
Table of Contents

Preface	xiii
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	37
Running a Bitcoin Core Node	38
Running Bitcoin Core for the First Time	39
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	51
C/C++	52
JavaScript	52
Java	52
Python	52
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	70
Implementing Keys and Addresses in Python	76
Advanced Keys and Addresses	80
Encrypted Private Keys (BIP-38)	80
Pay-to-Script Hash (P2SH) and Multisig Addresses	81
Vanity Addresses	82
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	153
Benefits of P2SH	154
Redeem Script and Validation	154

Data Recording Output (RETURN)	155
Timelocks	157
Transaction Locktime (nLocktime)	157
Check Lock Time Verify (CLTV)	158
Relative Timelocks	160
Relative Timelocks with nSequence	160
Relative Timelocks with CSV	162
Median-Time-Past	162
Timelock Defense Against Fee Sniping	163
Scripts with Flow Control (Conditional Clauses)	164
Conditional Clauses with VERIFY Opcodes	165
Using Flow Control in Scripts	166
Complex Script Example	167
8. The Bitcoin Network.....	171
Peer-to-Peer Network Architecture	171
Node Types and Roles	172
The Extended Bitcoin Network	173
Bitcoin Relay Networks	176
Network Discovery	176
Full Nodes	180
Exchanging “Inventory”	181
Simplified Payment Verification (SPV) Nodes	183
Bloom Filters	185
How Bloom Filters Work	186
How SPV Nodes Use Bloom Filters	189
SPV Nodes and Privacy	190
Encrypted and Authenticated Connections	191
Tor Transport	191
Peer-to-Peer Authentication and Encryption	191
Transaction Pools	192
9. The Blockchain.....	195
Introduction	195
Structure of a Block	196
Block Header	197
Block Identifiers: Block Header Hash and Block Height	197
The Genesis Block	198
Linking Blocks in the Blockchain	200
Merkle Trees	201
Merkle Trees and Simplified Payment Verification (SPV)	207
Bitcoin’s Test Blockchains	207

Testnet—Bitcoin’s Testing Playground	208
Segnet—The Segregated Witness Testnet	210
Regtest—The Local Blockchain	210
Using Test Blockchains for Development	211
10. Mining and Consensus.....	213
Introduction	213
Bitcoin Economics and Currency Creation	215
Decentralized Consensus	217
Independent Verification of Transactions	218
Mining Nodes	219
Aggregating Transactions into Blocks	220
The Coinbase Transaction	221
Coinbase Reward and Fees	223
Structure of the Coinbase Transaction	224
Coinbase Data	225
Constructing the Block Header	227
Mining the Block	228
Proof-of-Work Algorithm	228
Target Representation	235
Retargeting to Adjust Difficulty	235
Successfully Mining the Block	237
Validating a New Block	238
Assembling and Selecting Chains of Blocks	239
Blockchain Forks	240
Mining and the Hashing Race	247
The Extra Nonce Solution	249
Mining Pools	250
Consensus Attacks	253
Changing the Consensus Rules	256
Hard Forks	256
Hard Forks: Software, Network, Mining, and Chain	258
Diverging Miners and Difficulty	259
Contentious Hard Forks	260
Soft Forks	261
Criticisms of Soft Forks	262
Soft Fork Signaling with Block Version	262
BIP-34 Signaling and Activation	263
BIP-9 Signaling and Activation	264
Consensus Software Development	266

11. Bitcoin Security	269
Security Principles	269
Developing Bitcoin Systems Securely	270
The Root of Trust	271
User Security Best Practices	272
Physical Bitcoin Storage	273
Hardware Wallets	273
Balancing Risk	273
Diversifying Risk	274
Multisig and Governance	274
Survivability	274
Conclusion	274
12. Blockchain Applications	275
Introduction	275
Building Blocks (Primitives)	276
Applications from Building Blocks	278
Colored Coins	278
Using Colored Coins	279
Issuing Colored Coins	280
Colored Coins Transactions	280
Counterparty	283
Payment Channels and State Channels	284
State Channels—Basic Concepts and Terminology	285
Simple Payment Channel Example	286
Making Trustless Channels	289
Asymmetric Revocable Commitments	292
Hash Time Lock Contracts (HTLC)	296
Routed Payment Channels (Lightning Network)	297
Basic Lightning Network Example	298
Lightning Network Transport and Routing	301
Lightning Network Benefits	303
Conclusion	304
A. The Bitcoin Whitepaper by Satoshi Nakamoto	305
B. Transaction Script Language Operators, Constants, and Symbols	317
C. Bitcoin Improvement Proposals	323
D. Segregated Witness	329

E. Bitcore.....	343
F. pycoin, ku, and tx.....	347
G. Bitcoin Explorer (bx) Commands.....	357
Index.....	361

