

CONTENTS IN DETAIL

PREFACE	xv
Acknowledgments	xvi
1	
WHAT IS BITCOIN?	1
Why Bitcoin Now?	2
The Benefits of Using Bitcoin	3
The Complexity and Confusion of Bitcoin	4
What's in This Book?	5
2	
BITCOIN BASICS	7
How Bitcoin Works in Simple Terms	8
Bitcoin Units	9
The Bitcoin Address	10
The Private Key	11
The Bitcoin Wallet	12
Creating Your First Bitcoin Wallet with Electrum	14
Acquiring Bitcoins in Your Wallet	16
Spending Bitcoins with Your Wallet	17
Bitcoin Addresses Generated by Your Bitcoin Wallet Program	19
The Blockchain	19
The Blockchain Lottery	21
Blockchain Forking	23
Transaction Confirmations, Double Spending, and Irreversibility	25
Mining Bitcoins	26
The Complexity of the Bitcoin System	27
3	
STORING YOUR BITCOINS SAFELY, SECURELY, AND CONVENIENTLY	31
Storing Your Private Key(s)	33
Hot Storage vs. Cold Storage	33
Personal vs. Hosted Wallets	34
Safety, Security, and Convenience	35
Storing Small Amounts of Bitcoins	35
Online Hosted Wallet Services	36
Online Personal Wallet Services	37
Personal Hot Wallet	37

Storing Large Amounts of Bitcoins	38
Paper Wallets.	39
Encrypted Paper Wallets	39
Offline Transaction Signing	40
Fragmented Private Keys and Multi-Signature Addresses	41
Special Mention: The Bitcoin Hardware Wallet	42
Special Mention: The Bitcoin Brain Wallet.	45
Choosing the Storage Method That’s Right for You	46

4 BUYING BITCOINS 49

Why Not Just Mine Bitcoins?	50
Ways to Buy Bitcoins	51
Buying Bitcoins the Easy Way	52
Authentication Factors	54
The Hassle of Converting Dollars (or Other Currencies) into Bitcoins	55
Buying Bitcoins with Coinbase	58
Buying Bitcoins the Efficient Way	62
Buying Bitcoins from a Currency Exchange	65
Buying Bitcoins the Fun and Futuristic Way	67
Step 1: Finding Someone to Buy From	67
Step 2: Deciding on a Meeting Place	68
Step 3: Handing Over the Money and Getting Your Bitcoins	68
Satoshi Square	70
Still Don’t See a Buying Option That Works for You?	71

5 LOST AT SEA: A CRYPTOGRAPHIC ADVENTURE 73

6 WHY BITCOIN IS A BIG DEAL 109

A Brief History of Digital Currencies	110
The Dawn of Bitcoin	112
Bitcoin’s First Four Years	113
Bitcoin’s Early Impact	115
The Future Potential of Bitcoin	116
What Are the Existential Risks to Bitcoin?	117
What Role Might Bitcoin Play in the Future?	121
The Dangers of Decentralized Digital Money	123

7 THE CRYPTOGRAPHY BEHIND BITCOIN 129

A Brief Cryptography Overview.	130
One-Way Functions.	131
Cryptographic Hash Functions Verify Information	132
Public Key Cryptography	133

Digital Signatures	135
Using Digital Signatures.	136
Why Bitcoin Needs Cryptography	137
Authorizing Transactions with Digital Signatures	137
Verifying the Validity of the Transaction History	138
Proof-of-Work in Bitcoin Mining	138
Extra Protection for Bitcoin Private Keys	139
Cryptographic Methods Used in Bitcoin	139
Cryptographic Hash Functions: SHA256 and RIPEMD160	140
Crowley and the Unfortunate Jelly-Filled Donut Incident.	141
Moving Around on a Line	145
Elliptic Curve Digital Signature Algorithm (ECDSA)	146
Signing a Bitcoin Transaction Using ECDSA.	154
The Security of Bitcoin’s Cryptography	158
Pseudocode for Elliptic Point Summation and Point Multiplication	159

8

BITCOIN MINING 161

Why Is Bitcoin Mining Needed?	162
A Parable of Two Generals	162
Applying the Parable to Bitcoin.	164
Preventing Attacks with Mining	166
Distributing New Currency with Mining	167
How Does Bitcoin Mining Work?	168
How Miners Solve a Block	171
Anatomy of a Block.	171
Pooled Mining	175
Bitcoin Mining for Profit	176
Theoretical Hash Rate Limits	178
Decentralization in Bitcoin Mining	179

8.5

THE STRANGE WORLD OF ALTCOINS 181

9

UNDERSTANDING THE DIFFERENT TYPES OF BITCOIN WALLETS 185

Wallet Software Design Fundamentals	186
Offline vs. Online Transaction Signing	186
Random Key Generation vs. Deterministic Key Generation (vs. Single Key Generation)	187
Full vs. Simplified Payment Verification	191
Other Common (and Not So Common) Bitcoin Wallet Features	195
Future Wallets	197
Which Wallet Is Right for You?	197
Additional Wallet Considerations.	197

10	
BITCOIN 2030	199
What Will a Bitcoin Be Worth in 2030?	200
Bitcoin Mining in 2030.	201
A Day in the Life of a Bitcoiner in 2030	202
The Bitcoin End Game	210

A
HELLO MONEY! A SIMPLE JAVASCRIPT PROGRAM **213**

The Meaning of “Easy”	213
Three Ways to Write Bitcoin Software	214
General Security Notes on Bitcoin Programming	215
Some Upbeat Notes on Bitcoin Security	216
Writing Your First Bitcoin Program in JavaScript.	217
Why Use JavaScript?	217
Bitcoin Core vs. BitcoinD	217
Preparing Your Machine for JavaScript Bitcoin Programming.	218
Installing Node.js	218
Installing node-bitcoin	218
Starting Bitcoin Core	218
For Mac Hackers	219
For Linux Folks	219
Hello Money!	220
Part 1: Initializing the Connection with Bitcoin Core	220
Part 2: The Main Loop	221
The Bitcoin Core JSON-RPC API	222
Running the Hello Money! App	222
Limitations of Writing Bitcoin Programs That Use JSON-RPC	223

B
BITCOIN PROGRAMMING WITH BITCOINJ **225**

The Best Programming Language for Connecting to the Bitcoin Network	225
Installing Java, Maven, and the BitcoinJ Library	226
Step 1: Installing Java	226
Step 2: Installing Maven	227
Step 3: Installing Git	227
Step 4: Installing BitcoinJ	227
Creating a Starter Project for hello-money	228
Writing the Code for hello-money	230
Declarations at the Top of the Program	231
Initializing Our Java Objects	231
Connecting to the Bitcoin Network	233
Listening for New Money.	234

Running and Testing the hello-money Java Program	235
Bye-Bye Money	236
Importing a Private Key	237
Sending the Money	238
Ensuring the Money Transmission	238
Running bye-bye-money	238
Gotchas When Using Wallets in BitcoinJ.	239
Conclusion	240

INDEX **241**