

Contents

About the Author	xi
Acknowledgments	xiii
Foreword	xv
Prologue	xviii
Preface	xix
PART ONE: INTRODUCTION AND ECONOMICS	1
CHAPTER 1	
Foundations	3
1.1 Decentralized	4
1.2 Open Source	6
1.3 Public Asset Ledger	8
1.4 It's Not Only the Currency, It's the Technology	9
CHAPTER 2	
Technology (Introduction)	11
2.1 Centralized Database	11
2.2 Addresses, Transactions	13
2.3 Distributed Database, the Blockchain	15
2.4 Wallets	17
2.5 The Different Meanings of Bitcoin	18
CHAPTER 3	
Economics	21
3.1 Medium of Exchange	22
3.1.1 Pros	25
3.1.2 Cons	26
3.2 Store of Value	27

v

3.2.1	Bitcoin as Investment	29
3.2.2	Pros	30
3.2.3	Cons	31
3.3	Unit of Account	32
3.4	Deflation	32
3.5	Volatility	33
3.6	Effect on the Financial Industry and Monetary Policy	35
3.7	Regulation	37
 CHAPTER 4		
	Business Applications	39
4.1	Money Transfer	39
4.2	Exchanges	40
4.3	Payment Processors	43
4.4	Web Wallets	43
4.5	Multisignature Escrow Services	45
4.6	Mining	46
4.7	ATMs	48
 PART TWO: BITCOIN TECHNOLOGY		
		49
 CHAPTER 5		
	Public Key Cryptography	51
5.1	Public Key Encryption	53
5.2	Digital Signatures	56
5.3	RSA	59
5.4	Elliptic Curve Cryptography	62
5.4.1	Elliptic Curve Summary	63
5.4.2	Elliptic Curve Theory	64
5.5	Other Cryptographic Primitives	71
5.5.1	Blind Signatures	71
5.5.2	Shamir Secret Sharing	72
5.6	Bitcoin Addresses	73
 CHAPTER 6		
	Transactions	77
6.1	Transaction Scripts	80
6.2	Pay-to-address and Pay-to-public-key Transactions	82
6.3	Multisignature (m-of-n) Transactions	84
6.4	Other Transaction Types	85
6.5	Transaction Signature	86
6.6	Pay-to-script-hash (P2SH)	89
6.7	Standard Transactions	92

CHAPTER 7

The Blockchain	95
7.1 Hash Functions	95
7.2 Time-stamp	99
7.3 Proof-of-work	101
7.4 The Blockchain	105
7.5 Double-spend and Other Attacks	113
7.5.1 Race Attack	115
7.5.2 Finney Attack	116
7.5.3 Transaction Spamming	116
7.6 Merkle Trees	117
7.6.1 Transaction Malleability	119
7.7 Scalability	120

CHAPTER 8

Wallets	123
8.1 Symmetric-key Cryptography	125
8.2 Offline Wallets	126
8.2.1 External Storage Media	127
8.2.2 Paper Wallets	127
8.2.3 Offline Devices	129
8.2.4 Hardware Wallets	130
8.3 Web Wallets	131
8.4 Brain Wallets	132
8.5 Deterministic Wallets	132
8.5.1 Message Authentication Code (MAC)	134
8.5.2 Hierarchical Deterministic Wallets	135
8.6 Multisignature Wallets	136
8.7 Vanity addresses	137
8.8 Simplified Payment Verification (SPV)	139
8.9 The “Payment Protocol” (BIP 70)	141

CHAPTER 9

Mining	143
9.1 Mining Technology	146
9.2 Pooled Mining	149
9.3 Transaction Fees	154
9.4 Selfish Mining	156

PART THREE: THE CRYPTOCURRENCIES LANDSCAPE **159****CHAPTER 10**

The Origins Of Bitcoin	161
10.1 David Chaum’s Ecash	162

10.2	Adam Back's Hashcash	163
10.3	Nick Szabo's bit gold and Wei Dai's b-money	164
10.4	Sander and Ta-Shma's Auditable, Anonymous Electronic Cash	165
10.5	Hal Finney's RPOW	167
10.6	Satoshi Nakamoto	168
CHAPTER 11		
	Alt(ernative) Coins	171
11.1	Litecoin	172
11.2	PeerCoin	173
11.3	Namecoin	174
11.4	Auroracoin	175
11.5	Primecoin	175
11.6	Dogecoin	176
11.7	Freicoin	177
11.8	Other Alt-coins	177
11.9	The Case For/Against Alt-coins	178
CHAPTER 12		
	Contracts (the Internet of Money or Cryptocurrencies 2.0)	183
12.1	Digital Assets	183
12.2	Smart Property	185
12.3	Micropayments	186
12.4	Autonomous Agents	187
12.5	Other Applications	189
	12.5.1 Crowd-funding	189
	12.5.2 External State Contract	190
	12.5.3 Contract for Differences	190
	12.5.4 Distributed Exchange	191
	12.5.5 Deposits	191
	12.5.6 Saving Addresses	192
12.6	Inserting Data into the Blockchain	192
12.7	Meta-coins	194
	12.7.1 Colored Coins	196
	12.7.2 Counterparty	197
	12.7.3 Ethereum	199
	12.7.4 Mastercoin	202
	12.7.5 Nxt	203
	12.7.6 Ripple	204
CHAPTER 13		
	The Privacy Battle	209
13.1	Network Analysis	209
13.2	Laundry Services	212

13.3	Greenlisting	213
13.4	Privacy-enhancing Technologies	214
13.4.1	CoinJoin	214
13.4.2	CoinSwap	215
13.4.3	Stealth Addresses	217
13.4.4	Merge Avoidance	219
13.4.5	Committed Transactions	220
13.5	Fully Anonymous Decentralized Currencies	221
13.5.1	Zero-knowledge Proofs	221
13.5.2	Zero-knowledge Proof of Graph 3-colorability	221
13.5.3	Zero-knowledge Proof for the Discrete Logarithm	223
13.5.4	Non-interactive Zero-knowledge Proofs	224
13.5.5	Accumulators	225
13.5.6	Zerocoin	226
13.5.7	Zerocash	228

CHAPTER 14

Odds and Ends **231**

14.1	Other Transaction Protocols	231
14.1.1	Micropayment Channels	231
14.1.2	Atomic Cross-chain Trading	232
14.2	Alternatives to Proof-of-work	233
14.2.1	Proof-of-stake	234
14.2.2	Proof-of-burn	236
14.3	Merged Mining	237
14.4	Side-chains	238
14.5	Open Transactions	240
14.6	Quantum Computing	242
14.7	Recent Advances in Cryptography	244
14.7.1	Homomorphic Encryption	244
14.7.2	Obfuscation	245

Bibliography **247**

Index **259**