Blockchain and Distributed Ledgers

Mathematics, Technology, and Economics

Alexander Lipton
Sila Money, USA & Hebrew University of Jerusalem, Israel

Adrien Treccani
METACO, Switzerland

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI • TOKYO

Contents

out the Authors xi
st of Figures xxi
st of Tables xxxiii
st of Abbreviations xxxvii
eface xliii

Background **1**

1.1 Introduction 1
1.2 Distributed ledgers in a nutshell 2
1.3 A retrospective view 7
1.4 A perspective view 9
1.5 Book's structure 10
1.6 Summary 10
1.7 Further reading 11

The Global Financial System and its Pain Points **15**

2.1 Introduction 15
2.2 Money in retrospective and perspective 15
2.2.1 The role of money 15
2.2.2 Money as objects 16
2.2.3 Paper money 19
2.2.4 Anti-counterfeiting measures 21
2.2.5 Money as records 24
2.2.6 Money and inflation 26
2.2.7 BIS taxonomy of money 26
2.2.8 Where does money come from? 26
2.3 How the financial system operates at the moment 28
2.3.1 Current situation 28
2.3.2 Challenges faced by the current financial system 30
2.3.3 Detailed analysis of money creation 33
2.3.4 Negative interest rates 37
2.3.5 Banking regulations and monetary stability 38
2.3.6 The pros and cons of the current system 38
2.4 Domestic payments 39
2.4.1 The protagonists 39
2.4.2 Settlement 39
2.4.3 Credit card payments 39

2.5 Cross-border payments . . . 41
2.5.1 Cross-border transactions and correspondent banking . . . 41
2.5.2 Forex trading . . . 43
2.5.3 Informal funds transfer systems . . . 44
2.6 Blockchain payments . . . 44
2.7 Summary . . . 46
2.8 Exercises . . . 47

3 A Primer on Cryptocurrencies and Distributed Ledgers 49

3.1 Introduction . . . 49
3.2 Distributed identity . . . 50
3.2.1 Legal identification . . . 50
3.2.2 Digital identification and wallets . . . 51
3.3 Decentralized network . . . 52
3.3.1 Client-server model . . . 52
3.3.2 Peer-to-peer model . . . 53
3.3.3 Network nodes . . . 54
3.3.4 Bootstrapping of a node . . . 55
3.4 Distributed ledger . . . 56
3.4.1 Permissioning framework . . . 56
3.4.2 Blockchain data structure . . . 56
3.5 Double spending . . . 58
3.5.1 Illustration in a centralized setup . . . 58
3.5.2 Illustration in a decentralized setup . . . 59
3.6 Network consensus . . . 60
3.6.1 Sybil attacks . . . 61
3.6.2 Digital work with a proof-of-work . . . 62
3.6.3 Building the chain . . . 63
3.6.4 Block rewards and miners . . . 63
3.6.5 A computational power race . . . 64
3.6.6 Difficulty under competition . . . 65
3.6.7 Forks and consensus chain . . . 66
3.6.8 The 51% attack . . . 67
3.6.9 Confirmations and finality . . . 69
3.6.10 The limits of proof-of-work . . . 69
3.6.11 Staking as an alternative to working . . . 70
3.7 Path to the after-Bitcoin . . . 70
3.7.1 Pizza day . . . 70
3.7.2 Silk Road . . . 71
3.7.3 Altcoins . . . 72
3.7.4 Ethereum and smart contracts . . . 73
3.7.5 Tokenization . . . 74
3.7.6 Initial coin offerings . . . 75
3.7.7 Decentralized finance and autonomous organizations . . . 76
3.8 Summary . . . 77
3.9 Exercises . . . 77

4 Essential Cryptographic Tools 79

4.1 Introduction 79
4.2 Symmetric key cryptography 81
4.2.1 Introduction 81
4.2.2 Caesar's cipher 82
4.2.3 Affine cipher 82
4.2.4 A simple substitution cipher 83
4.2.5 The Vigenère cipher 83
4.2.6 The Enigma machine 83
4.2.7 A one-time pad 85
4.2.8 A stream cipher 85
4.2.9 Data encryption standards 86
4.3 Asymmetric key cryptography 86
4.3.1 Introduction 86
4.3.2 Cryptographic one-way functions 88
4.3.3 Abstract encryption-decryption algorithm 88
4.3.4 Abstract digital signature algorithm 88
4.3.5 Abstract secret-sharing algorithm 89
4.4 Elements of number theory 90
4.4.1 The set of integers modulo n 90
4.4.2 The Euclidean algorithm 90
4.4.3 The extended Euclidean algorithm 91
4.4.4 Fermat's little theorem 91
4.4.5 Euler's theorem 92
4.5 Finite ring cryptography 92
4.5.1 Modular exponentiation 92
4.5.2 A good trapdoor function? 93
4.5.3 A good trapdoor function! 93
4.5.4 RSA encryption-decryption algorithm 94
4.5.5 RSA digital signature algorithm 94
4.5.6 Blind digital signature algorithm 96
4.5.7 Chaum's anonymous cash 97
4.6 Finite field cryptography 98
4.6.1 Definitions 98
4.6.2 Primitive roots 99
4.6.3 ElGamal encryption algorithm 100
4.6.4 ElGamal digital signature algorithm 101
4.6.5 Schnorr digital signature algorithm 103
4.6.6 Diffie-Hellman key exchange 105
4.7 Elliptic Curve Cryptography 106
4.7.1 Continuous elliptic curves 106
4.7.2 Historical aside 108
4.7.3 Addition on elliptic curves 111
4.7.4 Projectivization of elliptic curves 115
4.7.5 Multiplication on elliptic curves 115
4.7.6 Discrete elliptic curves 116
4.7.7 The discrete log problem on elliptic curves 120
4.7.8 The standard elliptic curve secp256r1 122
4.7.9 Elliptic curve digital signature algorithm 123

4.7.10 Elliptic curve Schnorr digital signature algorithm 125
4.7.11 Diffie-Hellman key exchange 126
4.8 Comparison of different digital signature algorithms 126
4.9 Cryptographic hash functions 127
4.9.1 Hash functions 127
4.9.2 Collision-resistant hash functions 127
4.9.3 Signatures and hash functions 128
4.9.4 Signatures and birthday attacks 128
4.9.5 The random oracle hash 129
4.9.6 A practical hash function 130
4.9.7 Search puzzles and hash functions 130
4.9.8 Other uses of cryptographic hash functions 131
4.9.9 Iterative hash function with padding 131
4.10 Secure hash algorithms 132
4.10.1 Background 132
4.10.2 MD5 132
4.10.3 SHA-256 134
4.10.4 RIPEMD-160 137
4.11 Merkle trees and hash pointers 138
4.11.1 Merkle trees 138
4.11.2 Hash pointers and chain signatures 138
4.11.3 Chain signatures combined with Merkle trees 139
4.12 Quantum-resistant cryptography 141
4.13 Summary 142
4.14 Exercises 143

5 Bitcoin — A Deep Dive **145**

5.1 Introduction 145
5.2 Bitcoin addresses 147
5.3 Transactions 153
5.3.1 Distributed ledger accounting 153
5.3.2 Bitcoin transactions and mathematical induction 155
5.3.3 Transaction structure 156
5.3.4 Transaction scripts 159
5.3.5 Transaction verification 161
5.3.6 Representative transactions 161
5.3.7 Transaction broadcast 169
5.3.8 The Coinbase transaction 171
5.4 The Bitcoin ecosystem 174
5.4.1 Full node 174
5.4.2 Simplified payment verification node 174
5.4.3 Wallet 175
5.4.4 Solo miners 175
5.4.5 Mining pools 175
5.4.6 Exchanges 176
5.4.7 Bitcoin tumblers or mixers 176
5.5 Mining 177
5.5.1 Consensus 177
5.5.2 How Bitcoin rewards miners? 179

5.5.3 How do miners mine? 184
5.5.4 Mining difficulty 187
5.5.5 Pooling of resources 190
5.5.6 Malicious attacks 193
5.5.7 Soft and hard forks 195
5.5.8 Growing blockchain by induction 196
5.6 Anatomy of Block 600,000 198
5.7 Bitcoin pros and cons 199
5.8 Summary 202
5.9 Exercises 202

6 Ethereum — A Distributed World Computer? 205

6.1 Introduction 205
6.2 Similarities and differences between Bitcoin and Ethereum 207
6.3 A more centralized protocol? 208
6.4 Ethereum account types 209
6.5 The Ethereum Virtual Machine 211
6.6 Transfers and smart contract calls 211
6.7 Consensus 214
6.8 Smart contracts 217
6.8.1 Definitions 217
6.8.2 Example — A forward contract 220
6.8.3 Advantages and disadvantages of smart contracts 221
6.8.4 Oracles 223
6.9 Applications of Ethereum smart contracts 224
6.9.1 Potential use cases 224
6.9.2 Tokens and token standards 224
6.9.3 Crowdfunding via initial coin offerings 226
6.9.4 Stablecoins 227
6.9.5 Automated market makers 227
6.9.6 Decentralized autonomous organizations 229
6.10 Summary 231
6.11 Exercises 232

7 Ripple — A Simple Solution to a Complex Problem? 233

7.1 Introduction 233
7.2 Ripple protocol 233
7.3 Applications 238
7.4 Summary 242
7.5 Exercises 242

8 Central Bank Digital Currencies and Stablecoins 243

8.1 Introduction 243
8.2 Narrow banks 244
8.2.1 A brief history 244
8.2.2 Possible designs of a narrow bank 246

8.3 CBDC 247
8.3.1 Central banks as issuers of CBDC 247
8.3.2 Narrow banks as issuers of CBDC 247
8.3.3 Technical considerations 248
8.4 Stablecoins 249
8.4.1 Background 249
8.4.2 Stablecoins fully collateralized with fiat 250
8.4.3 Coins partially collateralized with fiat 252
8.4.4 Coins (over)collateralized with crypto 253
8.4.5 Dynamically stabilized coins 254
8.5 Digital trade coins collateralized with assets 256
8.5.1 General considerations 256
8.5.2 How to build a DTC 257
8.6 Summary 259
8.7 Exercises 259

9 Wallets and Key Management 261

9.1 Introduction 261
9.2 General wallet architecture 264
9.2.1 Necessary components 264
9.2.2 Network node 264
9.2.3 Blockchain indexer 265
9.2.4 Wallet application 266
9.2.5 Keystore 266
9.3 Wallet genesis 267
9.3.1 Key space 267
9.3.2 Brain wallet 268
9.3.3 The need for entropy 270
9.3.4 A concrete collision attack 270
9.3.5 True random number generators 271
9.4 Deterministic key derivation 272
9.4.1 The need for multiple keys 272
9.4.2 The original Bitcoin Core approach 272
9.4.3 BIP32 272
9.4.4 BIP44 277
9.4.5 Extensions to BIP32 278
9.5 From mnemonic to seed 279
9.5.1 Export and human-readability 279
9.5.2 BIP39 279
9.6 The relativeness of security 282
9.6.1 Custodial wallet services 282
9.6.2 A practical example 283
9.6.3 The Binance hack 284
9.6.4 The QuadrigaCX fraud 285
9.7 Key isolation and transaction approval 286
9.7.1 Security ingredients 286
9.7.2 Hot and cold storage 286
9.7.3 Four-eyes principle 287
9.7.4 Off-chain validation 287

9.7.5 On-chain validation 288
9.7.6 Multi-party computation 288
9.8 Summary 289
9.9 Exercises 289

10 Cryptocurrencies and Quantitative Finance 291

10.1 Introduction 291
10.2 Can cryptocurrencies be viewed as money? 292
10.3 Do fair prices of cryptocurrencies exist? 292
10.4 Distribution of daily BTC returns 293
10.5 Distribution of yearly BTC returns 306
10.5.1 The Fourier transform 306
10.5.2 Monte Carlo simulations 310
10.6 Distribution of daily ETH, XRP, and MRKT returns 311
10.7 Comparative statistics of cryptocurrency returns 325
10.8 Cryptocurrency ecosystem and its ecology 328
10.9 BTC valuation models 330
10.10 Bitcoin dominance index 339
10.10.1 The SIR model 339
10.10.2 The SIS model 340
10.11 Automated market makers 344
10.12 Summary 353
10.13 Exercises 353

11 Current Research Topics 355

11.1 Introduction 355
11.2 Intra- and interoperability 356
11.2.1 Background 356
11.2.2 Intraoperability 356
11.2.3 Interoperability 357
11.3 Privacy 360
11.3.1 Background 360
11.3.2 Payment channels 361
11.3.3 Coin mixing 362
11.3.4 Built-in cryptographic obfuscation 364
11.4 Scalability trilemma 365
11.4.1 Background 365
11.4.2 Current transactional banking model: scalable + secure 366
11.4.3 Current crypto model: decentralized + secure 367
11.4.4 Future fintech model: decentralized + scalable + secure 367
11.5 Summary 374
11.6 Exercises 374

12 Present and Future of DLT 377

12.1 Introduction 377
12.2 Financial Services 379

12.2.1 Accounting and audit 379
12.2.2 Global payments 382
12.2.3 Progammable money 384
12.2.4 Regulations 387
12.2.5 Trade execution, clearing and settlement 388
12.3 Government 390
12.3.1 Identity 390
12.3.2 Voting 394
12.4 Healthcare 396
12.4.1 Electronic health records system 396
12.4.2 Research 398
12.4.3 Supply chain 399
12.5 Supply chain 400
12.5.1 Supply chain management 400
12.5.2 Trade finance 401
12.6 Tokenization of real assets 403
12.7 Summary 404
12.8 Exercises 405

Bibliography *407*
Name Index *425*
Subject Index *427*