Index

A
Algorithm, 34
All-or-nothing approach, 138
Application layer, 4–5, 10
  functional aspects
    clarifying ownership, 192
    transferring ownership, 192
  nonfunctional aspects
    availability, 193
    censorship proof, 193
    open, 193
    pseudoanonymous, 193
    reliable, 193
Asymmetric cryptography, 190
  authorize transactions, 100
  complementary keys, 96
  create and distribute keys, 98
  decrypt cypher text, 97
  identify users, 99
  private to public, 99
  public to private, 99
  schematic illustration, 97
Auditing, 227
Authentication, 43–44
Authoritative chain, 168, 174–177
Authorization, 43–44, 68
Automation, 243

B
Bakery, 183
Bank account, 21

Bank notes, 50
Beaten paths, 165, 167
Behavioral integrity, 6
Bitcoin system, 187
Black key, 97
Block, 34, 160
  hash, 120
  header, 139, 156
  reference, 130–131
Blockchain
  -algorithm
    competition, 157–158
    identical working rhythm, 159
    metaphor used, 191
    peer control, 158
    punishment, 157
    purpose, 191
    reward, 156
    validation rules, 156
  -data-structure
    block header reference, 130–131
    book, 113
    comparison, 118
    content, 115, 120
    content reference numbers, 120
    get rid of spine, 117
    intended vs. unintended changes, 132
    mental unit, 119
    Merkle root, 129–130
    Merkle tree, 128
    metaphor used, 191
    new transactions, 125–126
    ordering catalog, 119

© Daniel Drescher 2017
D. Drescher, Blockchain Basics, DOI 10.1007/978-1-4842-2604-9
Index

Blockchain (cont.)
- orderly, 131–132
- page dependency explicit, 113–114
- page reference numbers, 120
- purpose, 191
- reference numbers, 117
- replace numbers, 116
- replace transaction, 128–129
- stores transactions, 120–121
- transaction data, 127
- layers, 192
- technical concepts, 190–191
- technology-suite, 200

Book
- get rid of spine, 117
- page
  - numbers, 114
  - order numbers, 115
  - preceding, 114
  - reference numbers, 117
  - replace numbers, 116
  - schematic illustration, 114

C

Card catalogs, 112

CDs, 19–20

Centralized software systems, 11, 15–16, 230

Chain
- consequences, authoritative
  - clarify ownership, 175
  - common trunk, 176
  - consistency, 176–177
  - orphan blocks, 174
  - reclaim reward, 175
  - robustness, 177
  - transactions reprocessing, 175
- heaviest-chain-criterion, 173–174
- longest-chain-criterion, 168–169, 171–172

Cloakroom tickets, 83, 86

Clock-pulse generator, 166

Collective decision-making problems
- characterize, 167
- conditions, 167

Collision resistant, 73

Combination lock, 89

Combined hashing, 76–77

Commercial concepts, 231

Common trunk, 176

Comparing data
- goal, 81
- idea, 82
- works, 82

Compensating peers, 186, 232

Compensation, 191

Complementary keys, 96–97

Compulsory data, 139

Computer science, 237

Computers gossip, peer-to-peer systems
- challenge, 146
- distribute new information, 149
- establish new connections, 149
- goal, 146
- introducing new peers, 147
- keep connections alive, 149
- news, 147
- overview, 147–148
- small talk, 147

Conceptual evolutions
- access rights, 238
- consensus, 239–240
- data structure, 241
- inventory data, 241
- privacy, 239
- transactions, 240–241

Concrete applications, 225–226, 228

Connecting pages, 118

Consensus, 167, 236, 239–240
- logic, 199

Content pages, 118, 120

Content reference numbers, 118, 120

Conventional mail, 93

Copying digital goods, 51–52

Cryptocurrencies, 227

Cryptography, 46, 59
- currency, 232
- hash functions, 72
  - collision resistant, 73
  - combined hashing, 76–77
  - deterministic, 72
hierarchical hashing, 78
independent hashing, 75
one-way function, 73
pseudorandom, 73
repeated hashing, 76
sequential hashing, 77–78
webpage, 73–74
hash value, 71, 74–75, 82, 86, 190
money, 186–187

Cryptology system, 94
asymmetric, 96–97
challenge, 94
goal, 94
idea, 94–95
metaphor, 93
symmetric, 96
terminology, 95–96

Cypher text, 95–97

D
Data, changes in
goal, 82
idea, 82
works, 82–83
Data integrity, 6
Data structure, 34, 241
Decentralization, 236
Delivery of messages, 148
Detecting changes,
comparing data, 83
Deterministic, 72
Digital assets, 227
Digital equivalent, 95
Digital identity, 227
Digitalization, 20, 22
Digital signatures, 100, 190, 196, 199
create, 105
identify fraud, 106–107
message verification, 105–106
requirements, 107
transaction data
combinations, 108
create, 107
verify, 108
Dishonest nodes, 137
Disintermediation, 22, 242
Distributed consensus, 167, 191
Distributed peer-to-peer system, 185, 230
metaphor used, 191
purpose, 191
Distributed software
systems, 217–218, 229
communication, 13
complexity, 14
computing power, 12
coordination, 13
cost reduction, 12
defined, 11
incremental growth, 13
mixing centralized and, 15–16
networks, 14
peer-to-peer systems, 23–24
reliability, 12
security, 14
Double spending problem, 50
copying digital goods, 51–52
peer-to-peer systems, 51–53
real estate, 50
solve, 52

E
E-mail, 94

F
Fingerprints, 71, 73
Formal correctness, 67
Four versions, 216
Functional\non-functional aspects, 5–6

G
Generic application, proof of
authorship, 226
existence, 225
identity, 226
nonexistence, 225
order, 225
ownership, 226
time, 225
Governmental projects, 247
Handwritten signatures, 103

Hash
  functions, 72
  puzzle, 142
    blockchain-data-structure, 140
    combination lock, 89
    difficulty level, 91
    elements, 89
    hash value, 90
    metaphor used, 191
    nonces, 91
    purpose, 191
    reward, 156
    role, 178–179
    schematic illustration, 90
    speed competition, 158
    works, 91–92
  references, 190
    after data alteration, 85
    invalid, 85
    refers, 84
    tree-like fashion, 88
    valid, 84

Heaviest-chain-criterion, 173–174

Hexadecimal numbers, 74

Hierarchical hashing, 78

Identical working rhythm, 159

Identification, 43–44

Immutability, 191
  aristocratic family, 135
  blockchain-data-structure
    all-or-nothing approach, 138
    compulsory data, 139
    computational costs, 138
    costs of manipulating, 141–142
    creating new block, 139–140
    making manipulations stand out, 138
    validation rules, 140
    works, 141
  challenge, 136
  data store in real world, 142
  defined, 137
  elements, 137
  goal, 136
  idea, 137
  metaphor, 135–136

Implementation layer, 4–5, 10
  functional aspects
    consensus logic, 199
    ownership logic, 195
    peer-to-peer architecture, 198
    storage logic, 197–198
    transaction processing logic, 196–197
    transaction security, 195–196
  nonfunctional aspects
    consistent, 194
    integrity, 194
    resilient, 194
    secure, 194

Independent hashing, 75

Integrity, 5–6, 30–31, 46, 52–53

Intermediaries, 21

Internet, 147

Inventory data, 64, 241

Jobs, loss of, 246

Knitting stitches, 123

Large-scale commercial projects, 247

Ledgers, 41–42, 44–45
  distribute, 60
    double spending problem, 51–52
    new transactions, 60–61
    transaction history, 61
    untrustworthy environment, 60

Legal acceptance, lack of, 209

Limited enthusiast projects, 246

Linked list, 87

Liquor shop, 42, 43

Longest-chain-criterion, 168, 170–173

Long-term accomplishments
  automation, 243
commodity, 244
cost reduction, 243
disintermediation, 242
processing speed, 243
security protocols, 244
standardization, 243
streamlining process, 243
technology awareness, 244

M
Mailbox, 93–94, 99
Mail, conventional, 93
Malicious peers, 31
Merkle root, 129–130
Merkle tree, 88, 120–121, 128, 141
Message, 148
delivery, 166
passing, 191
Micropayments, 227
Mobile phone
application vs. implementation, 4
element of layers, 5
functional vs. nonfunctional aspects, 5
integrity, 6
mental partition, 4
Multiple-choice tests, 153–154
Music industry
CDs, 19
digitalization, 20
Napster, 20
peer-to-peer systems, 21
studios, 20

N
Networks, 14
Nodes, 11, 15, 23, 30, 60
Nondiscrimination, 236
Notary services, 227

O
One-way function, 73
Openness, 236
Open peer-to-peer system, 185
Ordering catalog, 118–120
Orphan blocks, 174
Ownership
challenge, 64
concepts, 42
describe, 59
foundations, 41–42
goal, 64
lawful owner, 104
logic, 195
management, 35–36
protecting, 59
transfer, 65
witnesses, 40

P
Page reference numbers, 120
Paved paths, 165
Paxos, 240
Payments, 227
Payment system, 10
Peer control, 158
Peer-to-peer architecture, 198, 217
Peer-to-peer systems, 15
bank account, 21–22
centralized, 23
computers gossip, 146–150
distributed software
systems, 14, 23–24
double spending problem, 51
goals, 207
integrity, 30
ledgers, 61
malicious peers, 31
managing ownership, 190
music industry, 20–21
technical failures, 31
trust, 30
umbrella term, 34
Performance-related compensation
consequences, 154
multiple-choice tests, 154
rules, 154
Permissioned and permissionless
blockchains, 216
Ping, 149
Pocket calculators, 244
Pong, 149
Preceding page, 114
Privacy, lack of, 206, 245
Private blockchains, 215
Private key, 98–100, 206–207
Protecting ownership, 59
Pseudorandom, 73
Public blockchains, 215
Public key, 98–99
Public-private-key cryptography.
   See Asymmetric cryptography

Q
Quality competition, 158

R
Raft, 240
Reading access, 216, 218
Read-only data, 137
Record management, 227
Reference
   numbers, 112, 115–118
Register, 41
Reintermediation, 246
Repeated hashing, 76
Responsibility, loss of, 245

S
Scalability, 238
Scrolls, 113
Security
   authentication, 43
   authorization, 43
   identification, 43
   integrity, 6
   vs. speed, 214, 216
   technical limitations of blockchain, 206–207
Semantic correctness, 67
Sensitive manner, data changes in
   referring, 83–85
   storing data, 86–88
Sequential hashing, 77–78
Small talk, 147
Smart contracts, 240–241
Software architecture, 10
distributed systems, 11
Speed competition, 158
Standardization, 243
Stitches, 123
Storage logic, 197–198
Storing data, 86
   goal, 86
   idea, 86
   works, 86–88
Streamlining process, 243
Studios, 20
Symmetric cryptography, 96
System integrity, 185

T
Tax, 227
Technical limitations
   centrality, 208
   costs, 207
   lack of flexibility, 208
   lack of privacy, 206
   overcoming, 210
   scalability, 207
   security model, 206–207
   size, 209
Technology suite, 34
Transaction
   data, 59–61, 65, 104, 190, 205
   authentication, 68
   challenge, 112
   defined, 64, 66
   formal correctness, 67
   idea, 112
orphan blocks, 175
rules, 159, 161–162
semantic correctness, 67
validation rules, 156
history, 168, 205
heaviest-chain-criterion, 173–174
longest-chain-criterion, 168–172
metaphor used, 190
purpose, 190
processing logic, 196–197, 199
security, 195–196, 199
Transparency vs. privacy, 214–215
Tree-data-structure, 172
Tree-shaped data structure, 242
Trust, 30

U
Umbrella term, 34
Universality, 236
User acceptance, lack of, 210

V
Validation rules, 140–141, 156
block headers, 156
transaction data, 156
Voting schema, 178–179

W, X, Y, Z
Writing access, 216, 218